COUNCIL OF THE EUROPEAN UNION

Brussels, 8 February 2013

6231/13 ADD 1

Interinstitutional File: 2013/0024 (COD) 2013/0025 (COD)

EF 24 ECOFIN 103 DROIPEN 15 CRIMORG 15 CODEC 282

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	7 February 2013
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SWD(2013) 21 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT *Accompanying the document* Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial systems for the purpose of money laundering, including terrorist financing AND Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds

Delegations will find attached Commission document SWD(2013) 21 final.

Encl.: SWD(2013) 21 final

EUROPEAN
COMMISSION

Strasbourg, 5.2.2013
SWD(2013) 21 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing

and

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds

{COM(2013) 44 final}
{COM(2013) 45 final}
{SWD(2013) 22 final}

COMMISSION STAFF WORKING DOCUMENT

Accompanying the documents

Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing

and

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfer of funds

Contents

I. INTRODUCTION

This impact assessment has been prepared with a view to the revision of the Anti-Money Laundering framework[1].

Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter referred to as the Third AMLD), sets out the framework designed to protect the soundness, integrity and stability of credit and financial institutions (FIs) and confidence in the financial system as a whole, against the risks of money laundering (ML) and terrorist financing (TF).

The objective of Regulation EC 1781/2006 on information on the payer accompanying transfers of funds (hereinafter referred to as the Fund Transfers Regulation) is to enhance the transparency of fund transfers of all types, domestic and cross-border, in order to make it easier for law enforcement authorities to track funds transferred electronically by terrorists and criminals.

The EU rules are to a large extent based on international standards adopted by the Financial Action Task Force (FATF)[2]. They have been adapted to fit to an EU context and, as the EU Directive follows a minimum harmonisation approach, the framework has been completed by rules adopted at national level[3].

The FATF has undertaken a fundamental review of the international standards, which culminated in the adoption of a new set of recommendations in February 2012[4], and which place an increased focus on the effectiveness of regimes to counter money laundering and terrorist financing. In parallel to the international process, the European Commission has undertaken its own review of the European framework. This review has comprised an external study published by the Commission on the application of the Third AMLD (hereafter the Deloitte study)[5], extensive contacts and consultations with private stakeholders and civil society organisations[6], as well as with representatives of EU Member State regulatory and supervisory authorities and Financial Intelligence Units (FIUs).

The results of the Commission's review were set out in a Report to the European Parliament and Council[7] adopted in April 2012. The Report analysed how the different elements of the existing framework have been applied and considered how the framework may need to be changed. The responses to the ensuing public consultation have indicated a need to introduce clarifications or refinements in a number of areas. A revision of the Directive would in any

---

1 The framework is described in section III.2

2 See Annex I Glossary

3 The Directive is part of a broader set of legislative measures aimed at the prevention of money laundering and terrorist financing (see section III.2. Box 2).

4 http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf

5 Final Study on the Application of the Anti-Money Laundering Directive, Deloitte, December 2010, http://ec.europa.eu/internal_market/company/docs/financial-crime/20110124_study_amld_en.pdf

6 In addition, 2 private sector stakeholder meetings were organised in 2011.

7 COM(2012) 168 final, Report on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, 11.04.2012.

case have been needed in order to update it in line with the revised FATF Recommendations, which in themselves represent a substantial strengthening of the AML/CFT framework.

The constantly changing nature of money laundering and terrorist financing threats, driven by the limitless ingenuity of criminals coupled with constant technological evolution of delivery channels, necessitates the periodic review, and where necessary revision, of the legal framework designed to counter such threats.

II. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

II.1. Procedural issues

The preparation of this impact assessment has involved close coordination across Commission services. An Inter Service Steering Committee (ISSC) on AML was set up in January 2012, to discuss initially the draft application report, and subsequently to discuss the preparation of the impact assessment. The ISSC comprised the following services: MARKT, HOME, JUST, SG, TAXUD, SJ, FPI, and ENTR. The ISSC met on 4 occasions.

Work on the IA began in March 2012 and has been conducted over a period of five months. The IA was submitted to the Impact Assessment Board on 27 July and discussed on 5 September. The Minutes of the last ISSC meeting were submitted to the IAB.

The comments received from the IAB resulted in the following main changes:

- Additional information has been included in the problem definition regarding important differences between certain aspects of Member States' anti-money laundering frameworks (with respect to different approaches to identification of the beneficial owner, different thresholds applied for cash transactions, differences between national penalty regimes for non-compliance with AML rules and the differences in application of AML rules to the gambling sector – beyond casinos);

- Further information has been added with respect to the main changes at international level;

- The presentation of objectives and analysis of policy options has been simplified;

- The analysis of impacts on SMEs has been strengthened;
- The chapter dealing with analysis and quantification of impacts has been strengthened, incorporating more data and in particular including a specific analysis of administrative burdens;
- Explanations have been provided regarding the choice to lower the threshold for cash transactions from €15,000 to €7,500;
- An explanation has been included as to why the delay for responses to the Commission's application report was set for a period shorter than the 12 week minimum standard for public consultation.

II.2.External expertise and consultation of interested parties

The Commission services have made substantial efforts to obtain evidence in this field and to ensure full engagement of the different stakeholders:

- Over the course of 2010, a study by **external consultants** Deloitte was carried out on behalf of the Commission to look into the application of the Third AML Directive. The study involved an extensive consultation of various stakeholders.

- Member State **regulators** have been closely associated throughout the process with the work to prepare revisions to the legislative framework through the Committee for the Prevention of Money Laundering and Terrorist Financing (CPMLTF).

- Member State **supervisors** have made important contributions via the European Supervisory Authorities' (ESAs) Anti Money Laundering Committee[8]. In particular, in 2011 they produced two important studies on beneficial ownership[9] and simplified due diligence[10].

- Representatives of Member State **Financial Intelligence Units** (FIUs) have been associated with the preparation of the legislative texts, and have via the FIU platform[11] in particular contributed ideas on how cooperation between FIUs could be improved, as well as how to strengthen available tools and powers.

- Over the course of 2011-2012, the Commission organised two **private sector stakeholder meetings**[12] in order to discuss issues in relation to the preparation of its application report on the Third AMLD[13], and the followed these up with a number of bilateral or **sectoral meetings** with private stakeholder groups and civil society organisations. Participating stakeholders included representative European organisations in the banking, insurance, payments, e-money, accountancy, real estate, legal and gambling sectors. Also invited were representatives of various **civil society** organisations who had expressed clear interest in money laundering/terrorist financing issues. The Commission also carried out a written consultation of private stakeholder

---

8 The Joint Committee of the European Supervisory Authorities´ Sub Committee on Anti Money Laundering (AML Committee, AMLC) assists the European Supervisory Authorities in a supervisory capacity, to ensure a consistent implementation of the EU law.

9 EBA, ESMA and EIOPA's report on the legal, regulatory and supervisory implementation across EU Member States in relation to the Beneficial Owners Customer Due Diligence requirements under the Third Money Laundering Directive [2005/60/EC], AMLTF/2011/05, http://eba.europa.eu/cebs/media/aboutus/News%20and%20Communications/JC_2011_096--AMLTF-2011-05---UBO-Report-.pdf

10 EBA, ESMA and EIOPA's Report on the legal and regulatory provisions and supervisory expectations across EU Member States of Simplified Due Diligence requirements where the customers are credit and financial institutions under the Third Money Laundering Directive [2005/60/EC], AMLTF/2011/07, http://eba.europa.eu/cebs/media/aboutus/News%20and%20Communications/JC_2011_097-AMLTF-2011-07---SDD-report-.pdf

11 The "EU Financial Intelligence Units' Platform" was set up in 2006 by the European Commission. It gathers Financial Intelligence Units from the Member States. Its main purpose is to facilitate cooperation among the FIUs.

12 On 11 February and 9 December 2011.

13 Report of the first meeting is available at: http://ec.europa.eu/internal_market/company/docs/financial-crime/20110218-report_en.pdf

and civil society representatives between 11 April and 13 June 2012, the main results of which are described in Box 1[14].

Box 1: Results of the Commission's public consultation

In April 2012, the Commission adopted a report on the application of the Third AMLD, and solicited comments from all stakeholders on its considerations.

In particular, the report focused on a number of identified key themes (including application of a risk-based approach, extending the scope of the existing framework, adjusting the approach to customer due diligence, clarifying reporting obligations and supervisory powers, enhancing FIUs co-operation etc.), which are central to the review of the Third AMLD. In addition, the annex to the report addressed a closely related matter, namely cross-border wire transfers.

During the consultation period the Commission received 77 contributions[15] from public authorities, civil society, business federations and companies in several fields (including financial services, gambling sector, liberal professions, real estate sector, trust and company service providers), representing a broad variety of stakeholders. Replies came from 15 EU Member States and from some countries outside the EU (e.g. Jersey). 21 of the 77 replies, i.e. 27%, were provided by pan-European organisations.

The overall results of the consultation point to a general confirmation of the issues and problems highlighted by the Commission's Report, as well as broad support for the proposed alignment to the revised FATF standards and for greater clarification in particular in the areas of data protection and how to apply the rules in cross-border situations. Analysis of the responses reveals a diversity of opinions, which reflect the different categories of respondents. However, the industry most directly concerned by AML compliance generally welcomed this review as an opportunity to improve the effectiveness of the AML/CFT regime. Civil society organisations have responded with similar views. The feedback statement is available at the following address: http://ec.europa.eu/internal_market/company/docs/financial-crime/072012_feedback_statement_en.pdf

14 While the Commission's minimum standard for consultation is 12 weeks, in this special case the period for consultation was shortened due to the urgent need to adopt proposals in 2012, ahead of the start of FATF's fourth round evaluation process, which will begin in 4th quarter 2013. Swift adoption of a Commission proposal is supported by Member States, and is the most effective way to provide clear guidance to Member States seeking to adapt their own frameworks in advance of the FATF's fourth round evaluation, and the best way of limiting the risk that Member States adopt national rules which might subsequently conflict with the revised EU rules. Although the consultation formally closed on 13 June, the Commission services took fully into consideration all responses received after the deadline (i.e. 15 responses).

15 Contributions will be available on the Commission website, unless confidentiality has been specifically requested.

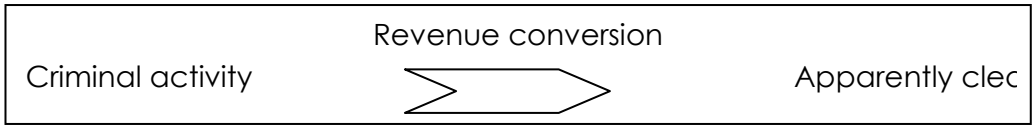
III. POLICY CONTEXT, PROBLEM DEFINITION AND SUBSIDIARITY

III.1. Background and context

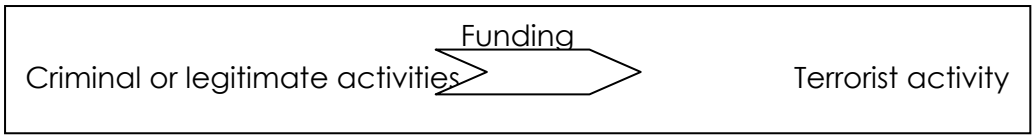
III.1.1. The nature of the problem of Money Laundering and Terrorist Financing.

Money laundering and terrorist financing are often subject to the same legislation. However, although the two concepts might share many elements, their defining features are quite different.

- **Money laundering** concerns activities related to assets which have a criminal or illicit origin. Criminals engaged in money laundering will therefore attempt to conceal or disguise the true nature, source or ownership of the assets in question and transform them into seemingly legitimate proceeds. If dirty money is allowed to flow through the financial system, the stability and reputation of the financial sector can be seriously jeopardised - which in turn could undermine the integrity of the single market.



- **Terrorist financing** on the other hand concerns the provision or collection of funds to carry out any of the offences defined in Council Framework Decision 2002/475/JHA on combating terrorism. Terrorist activities can be funded through legitimate as well as criminal activities and terrorist organisations engage in revenue-generating activities which in themselves may be, or at least appear to be, legitimate. There is a clear risk to the integrity, proper functioning, reputation and stability of the financial system, and with potentially devastating consequences for the broader society.



III.1.2. Nature and size of the market concerned

Obligations stemming from the EU's Third AMLD are applied not only by financial institutions (banks, insurance companies, the securities sector, etc.), but the framework extends beyond the traditional financial sector and covers gatekeepers of the financial system (auditors, external accountants, tax advisors, notaries, lawyers, real estate agents, casinos). Together, the combined sectors falling under the scope of the AML/CFT regime amount to nearly 10 million employees.

Compliance with AML/CFT rules has significantly different impacts according to the type of obliged entity. Large multi-national financial institutions may employ hundreds of thousands of staff, but there are also many small and medium-sized financial institutions, often active only at a local/domestic level. Persons working in the professional business services sector (lawyers, notaries, accountants, auditors, etc.) may be part of large cross-border groups, or

may work as independent professionals in small offices. The ML/TF risks associated with each business, and consequently the compliance burdens resulting from application of AML/CFT rules, will vary in accordance with the type of activity, the type of client and the geographical location[16].

In view of these differences between sectors, it is not possible to provide general data regarding how many staff work on compliance issues, and how many of those are specifically engaged in AML/CFT compliance. Some indications as to the costs of compliance are provided in Annex V on a sector by sector basis, along with additional background information including a general description of each sector as well as some typologies of money laundering and terrorist financing.

III.1.3. Main stakeholders affected by Money Laundering and Terrorist Financing

Table 1 Main stakeholders affected by Money Laundering, Terrorist Financing and the necessary countermeasures (under the baseline scenario)

Who is affected?		How?
1. Obliged entities	• Credit and Financial institutions • Auditors • External accountants • Tax advisors • Notaries • Independent legal professionals (involved in transactions) • Trust or company service providers • Real estate agents • Casinos • Other natural/legal persons trading in goods when cash payments >€15,000	*They are required to implement the rules, identify and verify the customer, the beneficial owner, understand the nature of the business relationship, conduct ongoing monitoring of the business relationship, file suspicious reports to FIUs, maintain records, and comply generally with the rules set out in the EU framework.*
2. Public authorities	• Regulators • Supervisors • Financial Intelligence Units • Law enforcement	*They are required to implement and enforce the rules and protect the system against criminal/ terrorist abuse*
3. Customers	Customers of the obliged entities (banks, financial institutions, auditors, etc.)	*They bear the burden of increased controls, reduced access to and increased cost of services.*
4. Business	Business community in general	*While increased controls and restrictions may complicate business transactions, an absence of effective AML/CFT regimes would increase risks associated with money laundering and terrorist financing – which would in turn be harmful to business interests*
5. Perpetrators	Criminals, terrorists, corrupt Politically Exposed Persons (PEPs)	*Are prevented from abusing the financial system, or can be traced and caught as a*

16 Annex IV contains an analysis of the costs of compliance with the Third AMLD from the perspective of different types of financial institution.

		result of the measures in place. However they are also quick to exploit any potential loopholes in the system.
6. EU Victims	EU Society/citizens	*Need to be protected from terrorist attacks, increased criminality, loss of welfare resulting from corruption, tax evasion, damage to market integrity, trust, etc.*
7. Non EU Victims	Society/citizens/governments in third countries	*Need to be protected against the EU financial system being used as a channel for illicit proceeds drained away from the local economy as a result of corruption and criminality.*

III.1.4. Impact of Money Laundering and Terrorist Financing

There is a general consensus globally and across political spectrums that immense damage can result if financial systems are insufficiently protected from criminal or terrorist abuse. In particular, systems which fail to prevent money laundering and terrorist financing expose themselves to:

- societal risk, stemming from the feedback of criminal and terrorist funds into criminal and terrorist activities;
- negative economic impacts, arising from disruptions to international capital flows, reduced investment and lower economic growth;
- financial market instability, resulting from reluctance of other financial intermediaries to engage in business, loss of reputation, drop in confidence and prudential risks.

III.2. Overview of legislative framework

EU legislators have put in place a preventative framework to combat money laundering and terrorist financing. The rules are to a large extent based on international standards, adapted to fit into an EU context. They are completed by rules adopted at national level:

Box 2: Overview of the main legal instruments in the field of AML/CFT

Directive 2005/60/EC (the "Third AMLD"):

- Prohibits money laundering and terrorist financing, and defines the types of conduct which are considered to constitute such offences. The Directive also defines the types of underlying criminal activity (i.e. the "predicate offence") which gives rise to the offences of money laundering or terrorist financing;

- Imposes an obligation on the "obliged entities"[17] to conduct "customer due diligence, (i.e. to carry out checks on customers in order to verify their identity, the identity of the beneficial owner[18], to understand the nature of the business relationship and to ensure that it is monitored on an ongoing basis). Should the obliged entity or person have knowledge or suspicion that money laundering or terrorist financing is being or has been committed, or attempted, they must promptly inform the Financial Intelligence Unit;

- Permits certain derogations from customer due diligence[19], by allowing for simplified procedure in certain listed cases[20]. Obliged entities must at least gather sufficient information to establish if the customer qualifies for Simplified Customer Due Diligence (SDD);

- Requires enhanced customer due diligence measures, for situations where there is a higher risk of money laundering or terrorist financing, such as where the customer has not been physically present for identification purposes, in the case of cross-border correspondent banking relationships with respondent institutions from third countries, and in the case of politically exposed persons residing in another Member State or a third country.

Directive 2006/70/EC (the "implementing Directive") lays down implementing measures for Directive 2005/60/EC as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

Regulation 1781/2006 on information on the payer accompanying transfers of funds: requires information on the payer to accompany transfers of funds, with the objective of ensuring prevention, investigation and detection of money laundering and terrorist financing. The Regulation covers all types of fund transfers carried out by electronic means in any currency, from a payer to a payee, which are sent or received by a Payment Service Provider (PSP) established in the EU (Art. 3.1). This is in order to make it easier for law enforcement authorities to track funds transferred electronically by terrorists and criminals.

A number of additional instruments which complete the framework are described in Annex II.

17 Article 2 of Directive 2005/60/EC imposes obligations on financial institutions, auditors, external accountants, tax advisors, notaries and other legal professionals (when participating in any financial or real estate transaction), trust or company service providers, real estate agents and casinos. There is also an obligation on other natural or legal persons trading in goods where payment is made in cash equal to or above €15,000.

18 Article 3(6) of the Third AMLD defines "beneficial owner" as the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted

19 The technical terms used in this Impact Assessment are explained in the glossary in Annex I

20 In the case of listed companies, beneficial owners of pooled accounts held by notaries and other legal professionals, domestic public authorities, certain types of life insurance policies, insurance policies for pension schemes and pension schemes – subject to certain conditions, and electronic money below €250 on a pre-paid, non-rechargeable device, or below €2,500 in the case of rechargeable devices.

III.3. Problem definition

III.3.1. Quantification of Money Laundering and Terrorist Financing

Given the illicit and hidden nature of money laundering and terrorist financing activities, no definitive figure can be provided which would accurately quantify the amounts processed by criminals for these purposes. As definitions differ as to which criminal activities (e.g. tax evasion) are considered "predicate offences" for money laundering purposes, comparison across countries can also be very difficult.

In recognition of the importance of providing policy-makers with better intelligence about the dimension of the problem, there have been efforts by international organisations to conduct research attempting to quantify the total amounts laundered across the globe. While any estimate must of course be treated with an appropriate degree of caution, there is general agreement that the amounts involved are very considerable.

The most widely quoted research dates back to the 1990s, when the International Monetary Fund (IMF), published a broad ranging estimate which quantified money laundering to be in the region of 2-5% of global GDP. In an EU context, if this range were extrapolated to the present day, with total EU GDP amounting to € 12.27 trillion, it could be assumed that the amount of money laundered funds was somewhere between € 245-613 billion (assuming an even distribution of money laundering globally).

More recent research has been published by the United Nations Office on Drugs and Crime[21]. The findings, which are broadly in line with the earlier IMF estimates, suggest that all criminal proceeds are likely to have amounted to some 3.6% of GDP or around US$ 2.1 trillion in 2009, with an estimated amount available for money laundering equivalent to some 2.7 % of global GDP, amounting to some US$ 1.6 trillion. With similar assumptions as above, the amount of money laundered annually in the EU could be estimated at around € 330 billion.

While the complex research methods used to calculate global amounts of money laundering can be contested and should not constitute a sole nor definitive basis for policy responses, more concrete illustrations of the vast sums at stake can be found in real life cases where money laundering has actually been detected, and where the facts are not open to dispute. Cases are many and varied, ranging from small scale operations, to huge schemes involving multi million or even multi billion euro amounts. The scale of money laundering uncovered in the case of Wachovia[22] (to date, the largest case of money laundering ever detected - see Annex V.1), serves as an important warning of the consequences that can arise in the event of a breakdown of AML defence mechanisms.

With respect to **Terrorist Financing,** no equivalent estimates of the overall amount of terrorist financing exist. According to a report of the UK House of Lords in 2009, however,

---

21 Estimating Illicit Financial Flows resulting from drug trafficking and other transnational organized crimes, UNODC, October 2011.

22 Between May 2004 and May 2007, wire transfers were made from Mexican currency exchange houses to Wachovia amounting to $373 Billion: there was no effective AML policy or procedure to monitor, detect and report suspicious wire transfers.

the mounting of terrorist operations appears – in contrast to the sums of money involved in money laundering – to involve much smaller amounts[23], while the detrimental impact they cause on society, on the economy and on security can be enormous, far exceeding the costs of mounting operations.

Box 3: Estimating the costs of mounting terrorist attacks[24]

Maintaining a terrorist network, or a specific cell, to provide for recruitment, planning, and procurement between attacks represents a significant drain on resources. A significant infrastructure is required to sustain international terrorist networks and promote their goals over time.

Nevertheless the direct costs of mounting individual attacks have been low relative to the damage they can yield, both financial and in terms of their societal impact. The only costs involved in domestic terrorism are those incurred in training and recruitment and the commission of the attacks.

For example, the 2005 London bombings were estimated to have cost just £8.000 (€ 10,000) sterling and Madrid train bombings costs were estimated to be $10.000 (€ 8,050).

Although the CIA estimated that Al-Qaeda had an annual budget of $30 million (€ 24 million) prior to 9/11 attacks in New York City, the total cost related to the preparation and execution of the attacks themselves was estimated to be no more than $500.000. (€ 400,000)

The vastly different sums of money implicated in money laundering and terrorist financing pose a particular challenge for regulators, financial institutions and gatekeepers of the financial system – on the one hand, vigilance is called for to keep the system safe against the possibility that it is used for the laundering of massive amounts of criminal proceeds, whilst on the other hand, mechanisms are needed to detect even the smallest amounts which might be used for terrorist purposes.

III.3.2. Areas most affected by Money Laundering and Terrorist Financing

The fight against money laundering has evolved over time. While the initial focus targeted the illicit proceeds of the drugs trade, the scope of crimes targeted by the AML/CFT framework has been progressively broadened to include the proceeds of fraud, corruption, and other crimes. The current EU framework takes an "all serious crimes" approach, and includes within its scope all other criminal offences which carry a punishment of imprisonment based on a mixture of maximum and minimum thresholds[25].

Similarly, while the framework initially included only credit and financial institutions, it has since been broadened to reflect the fact that other "gatekeepers" have an important role to play in preventing the system from being abused by criminals and terrorists. Money laundering can take many different forms, and beyond the banking sector, money laundering schemes have been detected involving lawyers, the real estate sector, the gambling sector, the insurance

23 House of Lords European Union Committee, Money laundering and the financing of terrorism, 22 July 2009

24 Various sources: FATF Report on Terrorist Financing (February 2008), UN Monitoring Team Report on Al-Qaeda and the Taliban (August 2004) and the Home Office (UK)

25 Article 3(5)(f) of the Third AMLD.

business – indeed all the sectors targeted by the legislative framework. Examples of money laundering according to each sector have been included in Annex V.

While it is difficult to provide estimates of the extent to which the various sectors are affected by money laundering, for the reasons described in the previous section, information is available about the extent to which the different sectors are filing reports. As with all data in this area, the figures must be treated with caution: the concept of a "suspicious transaction or activity report" can differ substantially across jurisdictions, as do the types of crime which give rise to a money laundering offence; the nature of the business relationship with a customer will also have an impact on the likelihood of reports being generated (each day, banks may be monitoring millions of transactions, while a lawyer or an accountant may only deal with a handful of clients); and given that financial institutions have been covered by the framework for considerably longer than other obliged entities, they have had more time to develop the experience and the systems to detect suspicious cases.

The following table is taken from the Commission's publication Money Laundering in Europe[26] and indicates the number of suspicious reports generated per sector in 2008. By far the largest number of filings are made by credit institutions and money transfer institutions. Reports from the non-financial sector are on the other hand much smaller by comparison, although there can be substantial variations across Member States.

[26] See Eurostat Working Paper *Money Laundering in Europe*, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-RA-10-003/EN/KS-RA-10-003-EN.PDF. Further explanations about the Commission's efforts to measure the effectiveness of the AML framework are described in Annex VII.

Table 2 Suspicious transaction reports according to sector

2008	Reporting FIUs	credit institutions	life insurance companies	investment firms	mutual funds	money transfer institutions	bureaux de change	lawyers	notaries	external accountants/ auditors	tax advisors	real estate agents	casinos	traders in goods above Euros 15000	trusts	company service providers	others	financial institutions	TOTAL
Member States reporting Suspicious Transaction Reports (STRs)																			
Belgium	STR	4 034	85	2	0	:	8 576	3	320	21	26	1	1 047	:	:	:	1 439	:	15 554
Bulgaria	STR	492	0	1	0	0	0	0	1	0	0	1	5	0	0	0	66	:	566
Czech Republic	STR	2 090	:	:	:	:	:	:	:	:	:	:	:	:	:	:	230	:	2 320
Denmark	STR	545	0	:	:	711	273	5	:	:	0	1	17	:	:	:	1	:	1 553
Germany	STR	6 352	37	0	0	920	0	9	5	3	5	0	4	9	0	0	5	:	7 349
Estonia	STR	3 028	2	1	0	2 130	41	6	53	3	0	0	37	23	0	0	522	2 432	8 278
Greece	STR	1389	:	204	:	322	37	:	:	:	:	:	:	:	:	:	272	:	2 224
Spain	STR	2 156	11	12	:	195	:	32	248	6	:	30	2	:	:	:	212	:	2 904
Italy	STR	11 242	179	15	:	1 265	0	6	103	5	36	13	4	:	20	:	6	:	12 894
Latvia	STR	21 266	26	0	0	414	0	3	4	0	0	0	0	0	0	0	2 250	:	23 963
Lithuania	STR	126	:	:	:	:	:	:	:	:	:	:	:	:	:	:	66	:	192
Luxembourg	STR	636	27	45	:	:	:	2	1	33	0	1	7	0	:	:	:	:	752
Hungary	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	61	1	:	62
Malta	STR	44	0	2	0	13	0	1	0	0	0	0	3	0	5	0	1	:	69
Austria	STR	992	8	:	:	:	:	6	3	1	:	3	:	8	:	:	38	:	1 059
Poland	STR	1 260	4	21	:	:	:	2	:	:	:	:	:	:	:	:	3	:	1 290
Portugal	STR	508	3	:	:	:	17	:	:	:	:	:	:	:	:	:	31	:	559
Romania	STR	1 545	5	3	:	17	1	2	225	:	:	2	12	51	:	2	468	5	2 338
Slovenia	STR	188	0	0	0	0	0	2	0	2	0	0	0	0	0	0	0	0	192
Slovakia	STR	1 942	261	0	0	0	0	0	5	1	0	0	0	49	0	0	17	:	2 275
Sweden	STR	7 232	0	5	:	1 452	4 177	:	:	2	0	0	145	:	4	1	30	:	13 048
Member States reporting Suspicious Activity Reports (SARs)																			
Cyprus	SAR	216	0	1	0	0	0	2	:	2	0	0	:	0	0	0	23	:	244
Finland	SAR	876	67	6	:	17 225	:	5	:	12	:	14	4 252	7	:	:	288	:	22 752
United Kingdom	SAR	202	:	909	:	8 438	3 524	6 319	:	7 104	97	170	:	41	:	48	25 984	168 620	221 466
Member States reporting Unusual Transaction Reports (UTRs)																			
Netherlands	UTR	5 013	13	:	0	288 799	0	16	568	112	7	0	538	53	4	:	341	:	295 464

III.4. Problem Drivers

The challenge for the AML/CFT framework is to ensure that the EU rules – and their enforcement – keep pace with evolving trends, developments in technology and the seemingly limitless ingenuity of criminals to exploit any gaps or loopholes in the system. The EU has in the past been at the forefront of the fight against money laundering and has set high standards for its framework. However, while that framework is designed to keep the system safe from criminal infiltration, there are unfortunately still many cases of money laundering (both in the EU and across the globe) which provide evidence that the problem of money laundering continues to plague the financial system[27]: it is a fair assumption that the cases identified represent only the tip of a very large iceberg. According to the October 2011 United Nations Office on Drugs and Crime (UNODC) study[28], the amount of funds intercepted by law enforcement is estimated to amount to less than 1% of the total funds laundered, and actual seizures amounted to less than 0.2%[29].

Assessing the extent to which countries' AML/CFT regimes may or may not be effective in safeguarding the system from money laundering or terrorist financing is complex. Some systems may encounter very low levels of corruption, and thus face reduced pressures to combat the problem. Other countries may be effective in facing up to ML/TF threats by having in place robust preventive and dissuasive measures which ensure that the number of cases of money laundering remains low. On the other hand, it may also be the case that countries faced with high risks of money laundering, but which have in place and weak preventive and enforcement systems, will be less able to identify and catch money laundering activity. Such considerations mean that any attempt to establish a link between non- or poor compliance with AML rules and higher incidences of recorded ML/TF cases will always remain problematic and can be misleading.

III.4.1. ***Problem Driver 1****: the existing rules are inconsistent with the recently revised international AML/CFT standards*

AML/CFT standards are agreed internationally and all EU Member States undergo a rigorous assessment process to ensure that their national legislation is in compliance[30].

In February 2012, new international standards were adopted by the FATF which are intended to enable national authorities to take more effective action against money laundering and

---

27 Recent cases of money laundering in the United States highlight the scale of the problem. In August 2012, Standard Chartered Bank reached a settlement with US authorities amounting to US$ 340 million, while Barclays Bank is understood to have set aside US$ 700 million to meet expected fines. Further examples of money laundering cases are described in Annex V.

28 Estimating Illicit Financial Flows resulting from drug trafficking and other transnational organized crimes, UNODC, October 2011

29 According to the UNODC study, the problem appears not to be a lack of international instruments, but shortcomings in the implementation of existing instruments in a number of jurisdictions. For that reason, focus at international level is increasingly on the evaluation of effectiveness of the systems, as opposed to straightforward compliance. This will be a key aspect of the FATF's fourth round evaluation process.

30 See Annex VI for further information about international standard setters (FATF and Moneyval) and section IX on the evaluation process.

terrorist financing at all levels – from the identification of bank customers opening an account through to investigation, prosecution and forfeiture of assets. They also better address the laundering of the proceeds of corruption and tax crimes and strengthen the requirements for higher risk situations and allow countries to take a more targeted risk-based approach.[31]

Box 4: Main Changes to the International Standards to combat Money Laundering and Terrorist Financing

There are many detailed changes resulting from the revision of the FATF standards which will require careful and detailed implementation into EU and national legal frameworks. The most significant changes for the purposes of this impact assessment are as follows:

Strengthening the risk-based approach: countries more at risk of money laundering or terrorist financing will need to do more than those less at risk. Countries need first to clearly understand the money laundering and terrorist financing risks which affect them, and adapt their Anti Money Laundering/Counter Financing of Terrorism (AML/CFT) system to the nature of these risks – with enhanced measures where the risks are higher and the option of simplified measures where the risks are lower.

Improving Transparency measures: the new standards have strengthened transparency requirements, requiring that there is reliable information available about the ownership and control of companies, trusts, and other legal persons or legal arrangements. More rigorous requirements on the information which must accompany electronic funds transfers will also be required. Measures to improve transparency, implemented on a global basis, will make it harder for criminals and terrorists to conceal their activities.

Towards more effective International Cooperation: With the increasing globalisation of money laundering and terrorist financing threats, the FATF has also enhanced the scope of international cooperation between government agencies (e.g. simplified extradition mechanisms), and between financial groups. The revised Recommendations will allow more effective exchanges of information, tracing, freezing, confiscation and repatriation of illegal assets.

Identification of clear Operational Standards: the FATF Recommendations concerned with law enforcement and Financial Intelligence Units have been expanded significantly. The revisions clarify the role and functions of the operational agencies responsible for combating money laundering and terrorist financing; and set out the range of investigative techniques and powers which should be available to them.

New threats & new priorities to be covered: The FATF also addresses new and aggravated threats and responds to the priorities set out by the international community, e.g. through the G20, in particular:

- ***Corruption & Politically Exposed Persons*** - i.e. people who may represent a higher risk of corruption by virtue of the positions they hold. The requirement to apply

[31] See FATF press release 16 Feb 2012, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html

enhanced due diligence to foreign politically exposed persons has been expanded with new recommendations also applying to domestic politically exposed persons and international organisations.

- ***Tax Crimes*** - The list of predicate offences for money laundering has been expanded to include tax crimes. Tax crimes are brought within the scope of the powers and authorities used to combat money laundering.
- ***Terrorist Financing*** – the FATF recommendations strengthen the requirements for tracking wire transfers, notably through the inclusion of information on the beneficiary in addition to the payer with the wire transfer. The scope for exemptions from the rules has been reduced.

There is a strong incentive on jurisdictions to correct inconsistencies with the international standards. Full compliance can send an important reputational signal which is vital for countries seeking to attract foreign investment. Non-compliance, on the other hand, is subject to an attentive follow-up process by the FATF or Moneyval. Persistent non-compliance can lead to inclusion in one of the **FATF's Public Statements**, which identify:

- Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures (e.g. entailing a need to apply enhanced customer due diligence to persons and institutions situated in those jurisdictions, etc…) apply and;

- Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

Inclusion in the FATF public statement can entail political and reputational damage for a country's financial sector leading to consequential economic costs resulting from loss of business, and can prove costly to remedy[32].

It is therefore essential to swiftly proceed with a revision of the EU framework to take account of the recent changes to the international standards. In particular, the EU framework is not, or is no longer compliant in the following key areas:

- **Risk-based approach:** the risk-based approach allows countries and obliged entities and persons to adopt a more flexible set of measures in order to comply with certain Recommendations. This helps them to target their resources more effectively and

[32] For example in October 2010, Greece along with a number of other countries, was placed on the FATF website, in the public statement under the title "Improving Global Compliance: on-going process". This resulted in administrative costs for the credit institutions established in Greece increasing - especially in the field of correspondent banking. The reputational effects of Greece's "grey listing" were most evident in the correspondent banking area. Correspondent banks, in isolated cases, lifted the simplified due diligence status for Greek banks. In some cases, following guidance from their supervisors or in accordance to their own internal policies, correspondents of Greek banks:
- sought KYC(Know-your-customer) information from their respondents' major shareholders/senior management;,
- declined to consider Greek banks as eligible third parties for the purpose of carrying out CDD for their local customers on their behalf;
- requested completion of "extended" Wolfsberg Group Questionnaires ; or
- required extra documentation for specific fund tranfers or trade financing transactions to which they had been involved.

apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way. Although the Third AMLD already includes some elements of a risk-based approach (e.g. in the case of CDD and risk-based supervision), the new FATF standards will broaden its application. In future, countries will be obliged, via a national risk assessment, to identify, assess and understand ML/TF risks, and to apply resources to mitigate those risks. There is also an acknowledgement that AML/CFT risk assessments at a supranational level should be taken into account, and that supervisors should apply a risk-based approach to supervision, based on their understanding of the ML/FT risks present in the country and within the entities they supervise.

- **Scope:** The new FATF standards have included "tax crimes (related to direct taxes and indirect taxes)" as a predicate offence[33], meaning that (at least serious) cases of tax evasion should in the future give rise to a money laundering offence, with a view to facilitating international cooperation and criminal prosecution. Although the Third AMLD[34] already sets out a range of "serious crimes" that are considered to be criminal activities, it does not specifically mention tax crimes[35].

- **Customer Due Diligence (CDD):** the application of the risk-based approach in the new FATF standards will require a more nuanced approach to the way in which situations requiring different levels of CDD are assessed. The current EU framework is based on a more prescriptive approach with respect to those areas to which enhanced due diligence (EDD) and simplified due diligence (SDD) must be applied. The increased emphasis on the risk-based approach in the revised standards reinforces arguments that the current EU approach needs to be changed.

- **Politically Exposed Persons (PEPs)**: PEPs[36], under the new international standards, are persons who have been entrusted with prominent public functions by foreign countries, or domestically, or by an international organisation. The current approach in the Third AMLD is to require EDD measures in the case of PEPs residing in another Member State or in a third country. The new international standards now introduce risk-based requirements for domestic PEPs, so that in future the new standards will apply different levels of obligation in respect of foreign and domestic PEPs, both as customers and beneficial owners of customers.

- **Beneficial Owners (BO)**: Under the Third AMLD, the BO means the natural person(s) who ultimately owns or controls the customer and/or the natural person on

---

33 This term is described in the glossary in Annex I

34 Article 3(5)(f) of the Third AMLD.

35 Indirectly however certain tax crimes are implicated through Article 3(5)(d) of the Third AMLD, which refers to "fraud, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests. The issue of how to improve responses to tax fraud is further considered in a Commission Communication adopted in June 2012: " Communication on concrete ways to reinforce the fight against tax fraud and tax evasion including in relation to third countries (COM(2012) 351 final)".

36 Article 3(8) of the Third AMLD defines "politically exposed persons" as natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.

whose behalf a transaction or activity is being conducted. Private stakeholders have expressed concerns that the existing EU rules[37] are in practice difficult to apply, and have called for further clarity and **better access to information**. The revisions to the international standards provide some additional clarity by setting out an approach for identifying and verifying beneficial ownership. The Commission's EU Internal Security Strategy (ISS)[38] also emphasises that understanding the criminal source of finances and their movements depends on information about the owner of the companies, as well as the trusts that those finances pass through. The ISS therefore proposes that the EU should consider, in the light of discussions with its international partners in the FATF, revising the EU AML/CFT legislation to enhance the transparency of legal persons and legal arrangements.

- **Third Country Equivalence**: The Third AMLD allows lighter CDD measures to be applied in the case of credit and financial institutions situated in EU/EEA countries. These lighter measures are extended to institutions situated in third countries which impose AML requirements considered to be "equivalent" to those laid down in the Directive. In order to co-ordinate their approach on equivalence, Member States have agreed on a regularly updated list of "equivalent third countries" in accordance with a Common Understanding on the Procedures and Criteria for the Recognition of Third Countries' Equivalence[39]. However the increased importance of the risk-based approach in the revised FATF Recommendations calls into question whether, going forward, the equivalence regime will remain appropriate at EU level. Given that country risk in the revised FATF Standards is only one of a number of factors[40], the continued relevance and usefulness of the equivalence list has been questioned.

- **Cross-border wire transfers**: the EU has fully implemented the existing FATF standards via a separate Regulation (1781/2006). This Regulation has the objective of making it easier for law enforcement authorities to track funds transferred electronically by terrorists or criminals by imposing obligations on ordering, intermediary and beneficiary financial institutions. The new FATF standards in particular include a requirement to include information about the beneficiary in wire transfers, and limit the possibility for exemptions from the information requirements (e.g. in the case of E-Money and mobile telephony fund transfers) There are specific obligations on money or value transfer service providers (MVTS), in particular a requirement to file a Suspicious Transaction Report (STR) in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Table 3 Summary of the main inconsistencies between the new FATF standards

37 Article 8(1)(b) of the Third AMLD requires, with respect to CDD obligations, identification of the BO and risk-based and adequate measures to be taken to verify his identity,

38 Commission Communication: "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM (2010)673 final.

39 http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-common-understanding_en.pdf

40 Other risk factors are: customer risk, product, service, transaction or delivery channel.

and current EU legislation		
Drivers	**New FATF standards**	**Current EU legislation**
Risk-based approach	Introducing national risk assessments and tailoring national approaches to the different types of risks faced. Greater emphasis on risk-based supervision. Greater emphasis on risk-based approaches for obliged entities.	• No requirement for national risk assessments, nor for coordination among EU Member States, nor for the development of supranational risk assessments • EU legislation will need to be adapted to more broadly apply risk-based approaches
Scope	Tax crimes now explicitly give rise to money laundering offence.	• EU legislation does not explicitly list tax crimes as a money laundering offence.
Customer Due Diligence	A more nuanced approach to the way in which situations requiring different levels of CDD are assessed is required. Need to consider a range of risk factors (e.g. customer risk, geographical risk, and product, service or delivery channel risk factors).	• EU legislation is currently prescriptive with respect to situations requiring/permitting SDD or EDD. • EU legislation currently lists possible exemptions from SDD.
Politically Exposed Persons	New risk-based requirements to identify domestic PEPs and PEPs working for an international organisation. The new standards will require obliged entities to ascertain whether the beneficiary of a life insurance policy is a PEP	• EU legislation currently only addresses foreign PEPs • EU legislation requires application of EDD measures for PEPs *residing* in another MS or a third country (not in conformity with standards) • EU legislation imposes a one year time limit after which persons who have ceased to be entrusted with a prominent function are no longer considered PEPs (not in conformity with standards), • EU legislation stipulates that "senior management approval" means the immediate higher level of the hierarchy of the person seeking the approval – this may not be appropriate in all cases.
Beneficial Owners	The new international standards set out an approach for identifying and verifying beneficial ownership, with measures aimed at finding a natural person with a controlling ownership interest, or (if none can be found or if there are doubts that the person with the controlling ownership interest is the beneficial owner) the natural person exercising control through other means.	• EU legislation requires identification by the obliged entity of the beneficial owner, but does not specify a means by which such information should be made available.
Third country equivalence	The risk-based approach in the new international standards calls into question the appropriateness of the equivalence regime of the EU - country risk is only one of a number of factors that obliged entities need to take into account.	• EU legislation allows lighter CDD measures to be applied in the case of credit and financial institutions situated in EU/EEA countries, which can be extended to institutions situated in third countries which impose AML requirements considered to be "equivalent" to those laid down in the Directive. • Member States have agreed on a regularly updated list of "equivalent third countries".
Cross-border wire transfers	The new international standards contain additional requirements for tracking transfers of funds, including information about the beneficiary of wire transfers. There are enhanced requirements with respect to verifying information.	EU legislation requires information only on the payer to accompany electronic fund transfers. EU legislation exempts fund transfers using E-Money and mobile phones below specific thresholds.

	The new international standards limit possible exemptions from the requirements There are specific obligations on money or value transfer service providers (MVTS), in particular a requirement to file a Suspicious Transaction Report (STR) in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit	EU legislation provides a possibility to exempt electronic money and fund transfers using mobile telephones below certain thresholds EU legislation requires filing of an STR to the FIU in whose territory the institution or person forwarding the information is situated.

*III.4.2. **Problem Driver 2**: the existing EU rules are differently applied across Member States leading to reduced legal certainty.*

In addition to the issues identified under Problem Driver 1, a number of areas have been identified[41] during the Commission's review process where the current EU rules result in inconsistent implementation. Such deficiencies cause uncertainties for businesses – especially those needing to ensure compliance in a cross-border context – and may impact on the effectiveness of the overall system to combat AML/CFT risks:

- Some concern has been expressed as to the **consistency of statistical data** relating to the effectiveness of AML/CFT systems[42]. Eurostat has collected a considerable amount of information relating to key indicators from FIUs[43], however there is recognition that significant definitional and systemic differences (e.g. different notions of what constitutes a "report", different processing of reports, different approaches towards prosecution of cases) considerably undermine comparability across countries and complicate effectiveness assessments of AML/CFT systems. As these differences between are the consequence of the different national approaches followed (e.g. what needs to be filed, when and how), it is impossible to rely on such information to draw any meaningful conclusions about the effectiveness of the system. Information received from Member States is therefore not sufficiently illustrative of the effectiveness of national AML/CFT systems.

- Article 3(6) of the Third AMLD defines "beneficial owner" as the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The Directive stipulates a 25% threshold of ownership or voting rights or, in the case of administered funds, the beneficiary of 25% or more of the property, for the identification of a "beneficial owner", for AML/CFT purposes. A report by the European Supervisory Authorities[44] has found that the way in which Member States determine how the **Beneficial**

41 The Commission has been made aware of these issues either because they have been highlighted in the Deloitte study, or as a result of contacts with (private and public) stakeholders.

42 Art. 33 of the Third AMLD sets out the minimum statistical requirements that Member States are obliged to collect.

43 See Eurostat Working Paper *Money Laundering in Europe*, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-RA-10-003/EN/KS-RA-10-003-EN.PDF

44 EBA, ESMA and EIOPA's Report on the legal, regulatory and supervisory implementation across EU Member States in relation to the Beneficial Owners Customer Due Diligence requirements under the Third Money Laundering Directive, AMLTF/2011/05, April 2012.

Ownership threshold should be calculated differs[45]. These differences may pose difficulties and increase costs at group level when designing customer identification procedures and assessing customer risk. They may also affect the level playing field for FIs and Designated Non-Financial Businesses and Professionals (DNFBPs) across Member States. Effective implementation has also been hindered by uncertainty amongst private sector stakeholders as to how to understand how far the obligation to "take adequate measures" to identify the beneficial owner needs to go in practice[46].

Box 5: Different approaches to the calculation of the 25% beneficial ownership threshold in EU Member States

According to the ESA's study, 13 MS broadly followed a "top down" approach with respect to the calculation of the beneficial ownership threshold, which means that in cases of indirect ownership, the percentage/share is determined by reference to the customer only. Some MS require institutions to determine whether a natural person at grandparent level (or beyond) holds 25% plus one share of the customer or more, e.g. a 30% share (grandparent level) of a 60% percent share (parent level) in the customer is considered an indirect 18% share in the customer and is not normally considered an ultimate beneficial owner. Other MS following the "top-down" approach, seeking to determine whether a natural person at grandparent level (or beyond) exercises control or owns at least 25% plus one share of the customer (de jure or de facto).

11 MS take the "bottom up" approach that ownership at any layer has to be counted in full, e.g. a 30% share (grandparent level) of a 60% percent share (parent level) in the customer is considered an indirect 30% share in the customer and thus a person who owns more than 25% of such entity is considered the ultimate beneficial owner.

- **Supervision:** Article 37 of the Third AMLD obliges Member States to require competent authorities to ensure compliance with the requirements of the Directive by all institutions and persons covered and to ensure that competent authorities have adequate powers – including to compel production of any information relevant to monitoring compliance and perform checks, and have adequate resources to perform their functions. Public stakeholders, especially supervisory authorities, have in particular expressed concerns about the lack of legal certainty in the current legislative texts about their ability to ensure correct compliance with host state AML/CFT obligations in the case of payment service providers, operating on the basis of a single EU passport via branches or agencies. Such uncertainties have the potential to create gaps in compliance and might undermine the effectiveness of the framework[47].

---

45 Certain Member States consider that the ultimate beneficial owner ("UBO") is the person(s) who owns/controls at least 25% of the customer, whilst other Member States interpret the UBO as the person(s) that owns/controls at least 25% of the customer, or of any entity that owns at least 25% of the customer. Other aspects of the definition give rise to uncertainties or different interpretations by Member States, in particular what "otherwise exercises control" over the corporate entity means in Article 3.

46 Article 8.1b of the Third AMLD states that Customer Due Diligence shall comprise "identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;"

47 In October 2011, the Commission services published a staff working paper entitled "Commission staff working paper on Anti-money laundering supervision of and reporting by payment institutions in various

- Article 39(2) of the Third AMLD obliges Member States to impose appropriate **administrative measures or sanctions** against credit and financial institutions for infringements of national provisions which stem from the Directive. The measures and sanctions must be effective, proportionate and dissuasive. While all Member States have been found to have implemented a national sanctioning regime applicable in cases of non-compliance with the provisions of the Directive, and that such sanctions are applied in practice, the Deloitte study concludes that "*the variety in national penalty regimes is so large that it is not possible to compare penalties through all Member States*"[48]. Different levels of sanctions can significantly impact the readiness of obliged stakeholders to comply with the Directive and to report suspicious transactions to the authorities, which can in turn impact the effectiveness of AML systems[49].

Table 4 Summary of the main differences across Member States and their Internal Market consequences

Rules differently applied by Member States	Description	Consequences
Consistency of statistical data on suspicious transaction reports	Significant definitional and systemic differences (e.g. different notions of what constitutes a "report", different processing of reports, different approaches towards prosecution of cases)	Reduced comparability of statistical data, difficulties to evaluate and monitor effectiveness.
Beneficial Ownership	Differences on how the beneficial ownership threshold should be calculated	Difficulties and costs for group AML compliance Negative impact on level playing field Uncertainty risks undermining effectiveness of group-wide AML
Supervision	Lack of legal certainty about supervisors' ability on host state obligations for branches and agencies	Gaps in compliance, reduced effectiveness of AML supervision Uncertainties for cross-border business
Administrative measures or sanctions	Differences in administrative measures and sanctions	Different incentives for obliged entities to comply with the AMLD via reporting, as a result, reduced effectiveness

cross-border situations", SEC (2011) 1178 final, http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm#report. The paper seeks to clarify how host state AML supervisory responsibilities resulting from the Third AMLD are to be understood in the context of home state supervisory responsibilities stemming from the Payment Services Directive.

48 See Annex VIII describing the differences between EU Member States' sanctions and penalties for non-compliance with AML/CFT rules.

49 For example, the Deloitte study (P.132) refers to an FATF report with regard to one EU Member State where (only) a low number of warning letters were sent by the supervisor (supervisor over a very large number of controlled entities) and concluded that in the absence of administrative fines, that it was unlikely that there was such a very high level of compliance with AML/CFT measures,

Box 6: Different levels of compliance with the international standards across EU Member States

The results of evaluations carried out by the FATF and Moneyval reveal some differences in the way that Member States have interpreted provisions in the Directive. For example, the requirements relating to Simplified Due Diligence in the Directive have generally been found to be overly permissive in evaluation reports. Within this, the provisions of the Directive have been interpreted differently, with some Member States considering the provisions to be an outright exemption, but others requiring at least some level of customer identification or ongoing monitoring.

*III.4.3. **Problem Driver 3**: Inadequacies and loopholes with respect to the current EU rules.*

Both the Commission's review process, and the revised FATF standards have identified inadequacies in the current framework. Under Problem Driver 3, the focus is on vulnerabilities or inadequacies which extend beyond those addressed by the revision of the international standards, but which appear important to address in an EU context:

- **Sports betting and other forms of gambling:** The Third AMLD includes "casinos" within its scope, but without providing any definition. The Directive also covers activities "performed on the Internet" (recital 14), thus covering on-line casinos. However as the Directive is based on minimum harmonization, national laws have addressed the broader risks associated with other forms of gambling in very different ways[50]. Private stakeholders have expressed concerns that some of the sectors most vulnerable to AML/CFT risks have not been covered by the legislation. In particular, increasing evidence is coming to light about money laundering risks linked to corruption in sport, and in particular match fixing. The FATF has published a Typology on the Football Sector[51] in which risks in betting activity related to the football sector have been identified.

- **Dealers in high value goods:** Dealers in high value goods fall within the scope of the Directive where the amount of the transaction exceeds €15,000 in cash, and are required by the Directive[52] to conduct customer due diligence for occasional transactions equal to or above that amount. Some Member States (see table) have taken a stricter approach towards the requirement for such persons to conduct CDD and either apply identification requirements as of a lower threshold, or else impose an outright ban on payments in cash above certain thresholds. The diversity of thresholds across Member States is at best confusing in an Internal Market context, but there is also a risk that such differences can lead to vulnerabilities in the borderless Schengen

50 See Annex IX, which illustrates the different coverage of MS laws in relation to casinos and the gambling sector.

51 Money Laundering through the Football Sector- July 2009.

52 Article7(b)

environment: the Commission has, for example, received complaints[53] that the proceeds of robberies and thefts committed in one Member State can be anonymously converted into cash in another Member State without any requirement to identify the customer if the amount of the transaction is less than €15,000.

Table 5	Member States with thresholds other than €15,000 for cash transactions, or imposing stricter requirements
BE	The following cash transactions are prohibited[54]: • Cash payment exceeding 5.000 EUR when purchasing one or more goods.
BG	CDD for cash transactions amounting to10.000 BGN or more (approximately 5.113 EUR) and a reporting obligation for any cash payment exceeding 30.000 BGN (approximately 15.339 EUR)[55].
DK	Retailers and auctioneers may not receive cash payments of DKK 100,000 (approximately 13.417 EUR) or more irrespective of whether payment is effected in one instance or as several payments that seem to be mutually connected[56].
FR	The following cash transactions are prohibited[57]: • Transactions over 3.000 EUR when the debtor has his place of residence in France or acting in a professional capacity; • Transactions over 15.000 EUR when the debtor does not have his place of residence in France or acting in a professional capacity and is not acting in a professional capacity.
IT	It is forbidden[58] to transfer cash, in euro or foreign currency between different persons when the value of the transaction, even if subdivided, is 1.000 EUR or more in total.
LV	Merchants dealing with precious metals, precious stones and articles thereof must report when a client pays cash in the amount of 10.000 Lats (approximately 14.100 EUR) and more.
RO	Payment operations between legal entities shall be made only by non-cash payment[59].
SI	Persons selling goods shall not accept cash payments exceeding 15.000 EUR from their customers or third persons when selling individual goods. This

53 See stakeholder response of Syndicat Saint Eloi (http://ec.europa.eu/internal_market/company/financial-crime/received_responses/responses-to-the-consultation/syndicat-saint-eloi_fr.pdf): over the course of 2011, 715 attacks were recorded against jewellery shops or precious metal dealers, as a result in the strong increase in the price of precious metals. In the absence of common thresholds for CDD, criminals can easily circumvent stricter national laws by crossing borders and laundering the proceeds of their crimes without any need for identification if the value of the transaction is below the €15,000 threshold.

54 Since 16 April 2012. As of 1 January 2014, this level will be further reduced to €3,000 euro for the sale of goods and service provision.

55 Article 11a of the Law on the Measures against Money Laundering.

56 Section 2 of Act on Measures to Prevent Money Laundering and Financing of Terrorism.

57 Article D112-3 j. L112-6 of Monetary and Financial Code.

58 Article 12(1) of d.lex 201/2011.

59 Government Ordinance 15/1996.

	includes legal entities and natural persons who organise or conduct auctions, deal in works of art, precious metals or stones or products thereof, and other legal entities and natural persons who accept cash payments for goods.[60]
Source: Study by consultants Deloitte on the Application of the Anti-Money Laundering Directive	

- **Financial Intelligence Units (FIUs)** – the Third AMLD requires each Member State to establish a Financial Intelligence Unit, to serve as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. The manner in which this goal is achieved is not stipulated in the Directive, with the result that the organisational nature of FIUs differs across Member States (they can be administrative, judicial, or police structures). The current framework for FIU Cooperation is based around a Council Decision dating back to 2000 ('the Decision')[61]. Discussions at the FIU platform[62] have revealed a number of shortcomings with the existing arrangements. Practical experience has demonstrated the types of problems that result from different interpretations about the legal basis granted by the Decision to undertake specific types of cooperation, such as the automatic exchange of information when links are found with another Member State. Some of the problems in exchanging information stem from the different powers that FIUs have at national level, including the possibility to access information, with consequences for the effectiveness of cooperation.

- **Group compliance/data protection**: Both public and private stakeholders have pointed to a number of difficulties as regards their compliance with AML/CFT requirements while ensuring a high level of **protection of personal data**. Under AML legislation, private stakeholders need to collect and process data (e.g. to monitor transactions and customer relations against sanctions lists, to apply an AML policy at group level, to identify beneficial owners, to maintain records for criminal investigation purposes, etc.). There is a lack of clarity about how these requirements are to be reconciled with rules on data protection, in particular at national level, which is leading to incoherent approaches across Member States. In 2009 a Commission Staff Working Paper[63] found evidence of problems relating to sharing of data across the group, including difficulties to organise identification/verification of clients centrally, difficulties to monitor cross-border activities of customers across the group, and difficulties to share information on suspicious transactions[64]. Clarification is

---

60 Article 37 of Prevention of Money Laundering and Terrorist Financing Act

61 Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

62 The "EU Financial Intelligence Units' Platform" was set up in 2006 by the European Commission. It gathers Financial Intelligence Units from the Member States. Its main purpose is to facilitate cooperation among the FIUs. .

63 Commission Staff working paper on "Compliance with the AML Directive by cross-border banking institutions at group level" SEC (2009) 939 of 30 June 2009. http://ec.europa.eu/internal_market/company/docs/financial-crime/compli_cbb_en.pdf

64 There is a clear link to problem driver 1, as the new FATF standards introduce a requirement (which largely mirrors work carried out by the Basel Committee on Banking Supervision) that financial groups must implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group.

therefore needed in order to enhance effectiveness of AML/CFT prevention, especially for businesses operating across borders, while ensuring a high level of protection of personal data. In 2011, European Data Protection Authorities issued recommendations providing guidance as to the application of data protection rules in the context of AML/CFT[65], some of which could already be helpful in clarifying AML legislation. In addition, the Commission is revising the European framework on data protection and published a set of proposals in January 2012[66].

III.5. Baseline scenario – How will the problem evolve without action?

Under the baseline scenario, the preventive system applied by financial institutions and designated non-financial businesses and professionals would remain in place, but would not be adapted in light of changes to the international framework nor in light of the findings of the Commission's own review process. In the short run, these would mean that no additional costs would be incurred by private stakeholders or public authorities. However in the medium to longer term, failure to adapt the rules would mean that:

a) the EU framework would not be in line with international standards (see Table 3), EU Member States would receive negative ratings for compliance by the FATF and their financial markets and institutions would suffer reputational damage. There would be a risk that, in the absence of new EU rules, any remedial actions taken individually by Member States at national level would result in fragmentation of the EU framework, uncoordinated regulatory responses and complications in particular for cross-border AML/CFT compliance by obliged entities;

b) The EU framework would remain predominantly rules-based, and would not take account of new emerging risks and threats. Difficulties for cross-border compliance resulting from different national rules would persist and undermine the Internal Market (see Table 4).

c) Failure to upgrade the AML/CFT system – and in particular failure to make better use of resources by strengthening the risk-based approach and placing more emphasis on the effectiveness of the framework – would leave the EU vulnerable to evolving threats arising from new business models and technologies. Deficiencies identified with the current rules as a result of the Commission's review process would not be corrected.

The consequences of the above shortcomings would lead to reduced effectiveness of the AML/CFT regime as well as negative reputational impacts[67], which would in turn:

---

65 Opinion 14/2011 of Article 29 WP.: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf

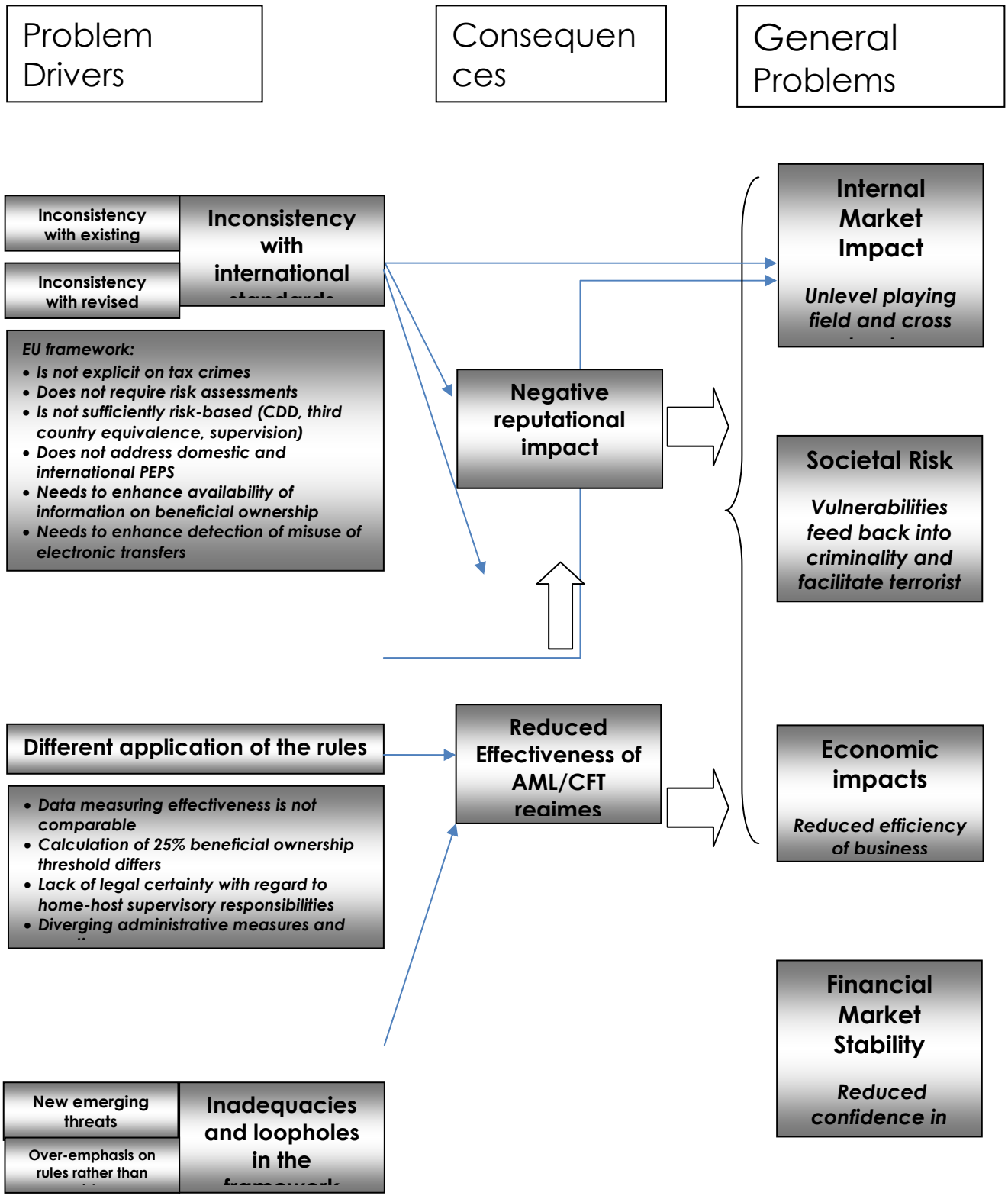
66 See the Commission's data protection proposals (COM(2012) 11 final) and (COM(2012) 10 final). http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

67 Countries go to great lengths to maintain high international standing with respect to their AML/CFT regimes, and suspicions of money laundering within a financial system can be hugely detrimental to investor confidence, and the willingness of foreign counterparts to engage in business transactions; this explains why in almost all cases, criticisms or public listing by the FATF are met with swift remedial responses.

a) *Impair the Internal Market:* in particular, the lack of coherence between national rules would make the organisation of EU cross-border business models more complex and burdensome;
b) *Negatively impact the stability of financial institutions and markets*: the reputational damage to the EU financial markets and financial institutions resulting from negative listings by the FATF would impair the ability of EU financial institutions to operate with other global counterparts – who would require evidence that the specific EU financial institutions had robust AML regimes in place despite poor FATF ratings of the EU framework.
c) *Negatively impact the EU economic situation*: reduced interconnectivity of the financial system would harm business interests – especially internationally;
d) *Generate societal risks* through increased ease of access by criminals and terrorists into the EU financial system: a system which, through lax controls, permits money laundering and terrorist financing is at risk that the proceeds of crimes are fed back into the system in order to fund additional criminal or terrorist activities.

These impacts are illustrated in the following problem tree.

III.6. Problem Tree



- ***Vulnerabilities with respect to traders in high value goods and in the gambling sector***
- ***Uncertainties with respect to data protection rules***
- ***Gaps affecting FIU cooperation***

III.7. The EU's right to act and justification

The Treaty on the Functioning of the European Union empowers the European Commission to act in the area of the Internal Market. In particular Articles 26 and 114 stipulate that "*the Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market*" and "*adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market*".

Member States have already recognized this need for action at EU level by adopting legislative measures in this area (see section III.2 and Annex II). Recital 2 of the Third AMLD states: "*The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to avoid Member States' adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy,* ***Community action in this area is necessary***."

Furthermore, according to the subsidiarity principle, the EU should act where it can provide better results than could be achieved by a response at Member State level. Recital 46 of the Third AMLD states that "*since the objective of this Directive [...] cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures,* ***in accordance with the principle of subsidiarity***".

As massive flows of dirty money and terrorist financing can damage the stability and reputation of the financial sector and threaten the internal market, any measures adopted solely at national level could have adverse effects on the EU Single Market: an absence of coordinated rules across Member States aimed at protecting their financial systems could be inconsistent with the functioning of the internal market and result in fragmentation. EU action is also justified in order to maintain a level playing field across the EU – with entities in all Member States subject to a consistent set of AML/CFT obligations[68].

The evaluation of the new international standards will begin in the fourth quarter of 2013. Unless the Commission provides clear and early indications of the desired EU approach to their implementation, there is a risk that those EU Member States who will be evaluated first will opt for solutions which may not coincide with the proposed EU approach, thus rendering agreement of common EU rules more difficult.

EU action should be limited only to what is necessary in order to attain the objectives, and must comply with the principle of proportionality. Several policy options are considered in Chapter V and in Annex III. The proportionality of each option has been analysed with regard

68 For example, different thresholds for applying customer due diligence in the case of cash transactions create vulnerabilities, e.g. lower thresholds are in place in some Member States aimed at controlling the sale of precious metals or stones and requiring identification of the seller. Criminals seeking to launder the proceeds of stolen goods can easily cross borders and sell the goods without the need for identification.

to its effectiveness. In all cases, the measures considered do not exceed what is necessary for the effective prevention of money laundering and terrorist financing.

The EU's right to act also needs to be examined in the light of the Charter of Fundamental Rights of the European Union ('the Charter'). The potential impacts of the proposal on Articles 2, 7 and 8 of the Charter (right to life, right of privacy and protection of personal data) are explained in detail in section VII.1 of this report.

Finally, with the adoption of revised international standards, commitments have been taken by the Commission as well as all EU Member States (either directly or via their membership of FATF or Moneyval) to ensure their implementation.

IV. OBJECTIVES

The overarching objectives for the revision of the AML framework are identical to those enshrined in the Third AML Directive and the Fund Transfers Regulation: protecting the financial system and the single market from abuse by criminals seeking to launder illicit proceeds, or from terrorists seeking to fund terrorist activities or groups.

The following **general objectives**, which in part reflect the objectives expressed in the recitals of the Third AMLD, are aimed at addressing the general problems identified in the problem tree:

1	Strengthen the Internal Market by reducing complexity across borders.
2	Safeguard the interests of society from criminality and terrorist acts.
3	Safeguard the economic prosperity of the European Union by ensuring an efficient business environment.
4	Contribute to financial stability by protecting the soundness, proper functioning and integrity of the financial system.

The **specific objectives** are linked more directly to the specific nature of the policy intervention:

1	Ensure that the AML/CFT framework meets high standards in order to safeguard the EU financial system.
2	Improve the effectiveness of AML/CFT regimes and thus protect the financial system and the single market from money laundering and terrorist financing.

The **operational objectives** are more specifically aimed at addressing the problem drivers identified in the problem tree:

Table 6 Operational Objectives

Problem Driver 1	Operational objective
Inconsistency with international standards • Assessment of the international standards have identified inconsistencies with the EU legal	Ensure that the EU approach is consistent with the approach followed at international level by extending the scope of application, strengthening and clarifying current requirements.

framework • The revision of the international standards in February 2012 requires that the EU framework be aligned to the new standards	
Problem **Driver 2**	**Operational objective**
• Existing rules of the Third AMLD are applied differently by Member States leading to reduced legal certainty	Ensure consistency between national rules and where appropriate flexibility in their implementation by strengthening and clarifying current requirements.
Problem **Driver 3**	**Operational objective**
• There are inadequacies and loopholes associated with the current EU rules.	Ensure that the rules are risk-focused and adjusted to address new emerging threats, by strengthening and clarifying current requirements.

V. POLICY OPTIONS: DESCRIPTION, COMPARISON AND IMPACTS

This section presents the policy options and their impacts for each policy area individually. Impacts are measured in terms of effectiveness (i.e. the extent to which they achieve the objective of the proposal), efficiency (notably cost-effectiveness) and coherence with other overarching objectives of EU policy.

V.1. Summary Description, Assessment and Comparison of the Main Policy Options

An important general issue to be addressed is the level of harmonisation to be achieved in order to meet policy objectives. Two approaches have been considered, with the preferred option being the one which would most appropriately fit to all the dimensions analysed in Table 7.

1. **Fully harmonise the framework**:

A number of stakeholders have called for a full harmonisation approach, which would entail the application of a single set of rules across the EU. Full harmonisation would represent the best way of achieving a consistent approach across the Internal Market, while implementing international standards. However, it would fail to ensure an appropriate degree of flexibility across Member States so that they can address the risks which are specific to their jurisdiction. This option would not therefore fully satisfy Operational Objective 2. Furthermore, by denying an appropriate degree of flexible implementation, a fully harmonised framework may also run counter to the risk-based approach, potentially leading to EU Member States being found non-compliant with the international standards. Although there would be cost advantages for cross-border businesses, there would most likely be significant adjustment costs needed for businesses operating only in domestic markets, who would gain no additional benefits from the single market. Full harmonisation across the board would therefore not be appropriate.

2. **Introduce additional elements of harmonisation in selected areas**:

This approach would allow Member States to maintain a necessary degree of flexibility in appropriate circumstances at national level, in recognition that this is the most effective way to address crime prevention and to ensure a tailored approach in certain areas. Targeted harmonisation can ensure that Member States are able to retain flexible approaches in certain areas (e.g. in the cases which call for the implementation of risked-based procedures), thus recognising that certain risks may be different across Member States. The harmonising approach also brings convergence of rules in other areas (e.g. modifying the scope in order to ensure a level playing field and to enhance the Internal Market, converging approaches to identify the beneficial owner, improving comparability of statistical data, etc.).

When adjusting the existing framework, each separate dimension under consideration needs to be assessed in light of how effectively it strikes an appropriate balance between *flexibility* and *convergence*. In the event that the balance is too far weighted in favour of a flexible approach, further consideration is needed with respect to mitigating elements, such as putting in place processes to ensure further convergence (e.g. by mandating European supervisors to publish guidance, or by including the possibility for elements of risk assessments to be conducted at EU level).

Thus framed, targeted measures to promote convergence should achieve a correct balance between promoting consistency while at the same time maintaining an appropriate degree of flexibility. The policy options corresponding to each dimension under Table 7 have been assessed with a view to achieving that correct balance, while – to the extent possible – meeting the operational objectives.

V.2. Main Policy Options Relating to the Operational Objectives

The assessment of policy options in this section represents a summary of the more detailed analysis of policy options contained in Annex III. The views of different stakeholders groups are systematically presented in the same Annex, when comparing the identified policy options. For reasons of simplicity, the policy options have been segregated according to the three different operational objectives. It is however clear that there are overlaps between the problem drivers and objectives and that certain of the changes under consideration could be viewed from various angles (e.g. adapting a risk-based approach in order to adhere to the international standards, while finding the right solutions from an Internal Market perspective). The "no change option" has been assessed in detail under the baseline scenario, and the analysis is not repeated here[69]. In most cases, the status quo would not be a realistic alternative, due to the consequences associated with non-implementation of the international standards.

The assessment of options is made extensively in Annex III to this Impact Assessment. Table 7 presents the results of that analysis in the form of each preferred option, as well as the alternative option that was assessed.

Table 7 Description, assessment and comparison of the main policy options

DIMENSIONS	***Policy Options relating to Operational Objective 1 (****Ensure that the EU approach is consistent with the approach followed at international level by extending the scope of application, strengthening and clarifying current requirements****).***	
	Preferred Options	**Alternative Options**
1. **Inclusion of tax crimes in the scope**	DESCRIPTION: include an explicit reference to tax crimes as a predicate offence. It would not provide a precise definition, but use the existing threshold approach applied in the case of serious crimes.	DESCRIPTION: include tax crimes as a specific predicate offence, and design detailed rules for the circumstances in which the offence is committed.
	ASSESSMENT: This option would achieve, in terms of effectiveness, efficiency and coherence, the objective set. It would bring about a degree of consistency across Member States, although some differences across jurisdictions would still remain. It would	ASSESSMENT: This would be the optimal option to achieve Internal Market goals. In terms of effectiveness it would ensure coherence across the EU, while sending a clear signal with respect to tax crimes. It would facilitate a more efficient environment for cross-

69 Except in the case of Dimension 10 (Home and Host Supervisory Responsibilities for AML), where the alternative option is in fact the baseline scenario.

	comply with the international standards and send a clear signal with respect to tax crimes.	border businesses and would be in line with international standards. It would however entail substantial delays due to political difficulties in agreeing a common list of types of tax evasion. This would result in delaying the agreement on the whole AML/CFT package and for these reasons it should not be retained.
COMPARISON: Effectiveness Efficiency Coherence	 +++ 0 +	 +++ 0 0
2. **National Risk Assessments**	DESCRIPTION: introduce a requirement for Member States to carry out a risk assessment at national level and take measures to mitigate risks. An option would also be introduced for supranational risk assessments to be undertaken in areas to be determined.	DESCRIPTION: treat the EU as a single jurisdiction and require a risk assessment to be carried out at EU level, prescribing actions to mitigate risks at EU level.
	ASSESSMENT: This option would meet the objective of strengthening the requirement to carry out national risk assessments. The approach would be fully in line with international standards, while recognising the specific supranational character of the European Union. It would give flexibility for Member States to recognise national differences.	ASSESSMENT: This option would result in greater convergence between Member States' approaches. It would bring about more legal certainty for obliged entities operating across borders. However a supranational risk assessment may be very costly and resource intensive. In terms of efficiency and coherence, such prescriptive rules may lead to less flexibility and adaptability, impairing effectiveness of AML regimes.
COMPARISON: Effectiveness Efficiency Coherence	 ++ + 0	 0 - - 0
3a. **Customer Due Diligence**	DESCRIPTION: Member States to ensure that EDD must be conducted in certain situations of high risk, while allowing them to permit SDD in lower risk situations. Determination of the level of risk would be based on examples of the factors to be considered (such as geography, customer type, delivery channel, etc.). Guidance on its application would be provided by EU bodies (e.g. ESAs and other appropriate EU bodies/agencies/committees).	DESCRIPTION: introduce prescriptive provisions into the Directive setting the conditions for applying EDD and SDD.
	ASSESSMENT: This option would facilitate a targeted approach to risk, resulting in better mitigation. Publication of guidance would ensure coherence of	ASSESSMENT: This option would ensure a consistent approach and a level of certainty. The current rules already include – to a certain extent –

	approach across EU Member States. It would be in line with the revised FATF standards. There could be short-term costs to implement systems, and differences of interpretation would still remain. However, the benefits appear to outweigh the disadvantages.	prescriptive rules for the application of EDD and SDD, in some cases left to Member State discretion. However this option would not be sufficiently flexible to deal with the changing nature of ML/TF risks. Moreover, it would require a resource-intensive EU-wide risk assessment in order to determine appropriate prescriptive provisions and would not allow Member States any flexibility to respond to specific risks that they might be facing.
COMPARISON: Effectiveness Efficiency Coherence	 + + 0	 0 - - 0
3b. **Equivalence of third country regimes**	DESCRIPTION: Remove the "white list" process. Countries deemed to have AML systems *not equivalent* to those in the EU are treated as a factor/example to be taken into account by obliged entities when considering geographical risk.	DESCRIPTION: completely remove the "equivalence" process, leaving Member States and obliged entities to make their own decisions about risks associated with third country regimes.
	ASSESSMENT: This option would ensure consistency of treatment of third countries across the EU, while recognising that some third countries do not meet high EU standards. It would allow the use of a risk-sensitive approach. However, different applications across EU Member States may remain.	ASSESSMENT: This option would arguably be the most risk-sensitive approach; it would avoid the concentration on one risk factor (i.e. geography). In contrast, in terms of coherence it would result in the least convergence of approaches across EU Member States.
COMPARISON: Effectiveness Efficiency Coherence	 ++ 0 0	 0 0 -
4. **Risk-Sensitive Approach to supervision**	DESCRIPTION: specific recognition in the Directive that supervision can be carried out on a risk-sensitive basis, with a role given to ESAs to develop more detailed measures.	DESCRIPTION: allow full discretion for supervisors to apply a risk-sensitive approach to supervision, without any additional measures at EU level.
	ASSESSMENT: This option would allow supervisors to adopt approaches which are more targeted towards risk. The concept would be appropriate in developed sectors (such as banking, securities and insurance supervision), and less so in certain DNFBP sectors where a sectorial approach at EU level might not be viable at present.	ASSESSMENT: This option would maximise flexibility for all supervisors, but would potentially lead to a lack of convergence as each sector in each Member State would be supervised according to different risks and principles.
COMPARISON: Effectiveness	 + +	 +

Efficiency Coherence	+ 0	0 0
5. **Treatment of Politically Exposed Persons**	DESCRIPTION: introduce new requirements for domestic PEPs/PEPs working in international organisations, with risk-sensitive measures to be taken. As not all such PEPs are automatically higher risk, a risk sensitive element would be introduced to allow obliged entities to assess the risks that they pose and to apply appropriate mitigating measures.	DESCRIPTION: require EDD for all types of PEPs (not just foreign PEPs).
	ASSESSMENT: This option would continue to address highest risks (foreign PEPs) and allow a graduated approach to other PEPs. However, the differential approach might cause some confusion for obliged entities, who would need to apply different standards to different categories of PEP. The approach is consistent with the international standard.	ASSESSMENT: By requiring a certain level of enhanced due diligence to be conducted for each category of PEP this option would give greater clarity and more consistency to the provisions, while placing the EU ahead of the international standard. It would however come with a high cost for industry, without a corresponding benefit.
COMPARISON: Effectiveness Efficiency Coherence	 + + 0 +	 + 0 -
6. **Availability of beneficial owner (BO)information**	DESCRIPTION: require all companies to hold information on their BO. This would need to be made available to competent public authorities and entities/ persons covered by the Directive.	DESCRIPTION: require Member States to set up public registries on shareholders, beneficial owners and nominees.
	ASSESSMENT: This option would allow greater transparency of information on the ultimate beneficial owner of companies. It would ensure coherence with Commission's policy and the international standards. Nonetheless, some cost would be necessary for recording and maintaining this information, and making it available upon request. It would meet the demands of the European Parliament and civil society, and assist entities and persons covered by the Directive in carrying out CDD.	ASSESSMENT: If properly implemented, this option would increase the level of transparency and would meet the demand from civil society and European Parliament. It would assist obliged entities. However, it would be a challenge to maintain up-to-date information and it would entail substantial costs for Member States.
COMPARISON: Effectiveness Efficiency Coherence	 + + ++	 + 0 0
7. **Electronic fund**	DESCRIPTION: amend the Fund	DESCRIPTION: require beneficiary

transfers	Transfers Regulation to reflect the new international standard by introducing a requirement to include information on the beneficiary to accompany the fund transfer, as well as limit exemptions from scope.	and payer information to accompany the payment as per the international standard, and require identity verification as of €0 (as opposed to the existing threshold of €1,000).
	ASSESSMENT: Ensuring that beneficiary information is included in all electronic fund transfers would provide an effective tool for law enforcement and ensure full traceability of all transfers. However, it would imply (limited) additional costs for business to adapt the payment systems.	ASSESSMENT: This option would be the most effective way of ensuring full traceability of electronic fund transfers, while exceeding international standards. In contrast, in terms of efficiency, it would entail significant additional costs for non-account based payment service providers.
COMPARISON: Effectiveness Efficiency Coherence	 + - +	 - - +
	Policy Options relating to Operational Objective 2 (*Ensure consistency between national rules and where appropriate flexibility in their implementation by strengthening and clarifying current requirements).*	
	Preferred Options	**Alternative Options**
8. **Comparability of statistical data**	DESCRIPTION: reinforce and make more precise the requirement under Art. 33 with respect to collecting and reporting statistical data in order to ensure more comprehensive and comparable statistics.	DESCRIPTION: provide further guidance on how reporting by Member States should be carried out with a view to achieving more coherence between data sets.
	ASSESSMENT: This approach would enhance comparability of important effectiveness indicators across the EU. It would be consistent with the international standards and in general with our objective. However, comparability across Member States would possibly remain impaired as a result of underlying differences with respect to AML approaches.	ASSESSMENT: This option improves the ability to measure effectiveness of the EU framework. It would be in line with the international standards. However, comparability across the Member States would remain difficult. Thus it would not be the best means to achieve the pursued objective.
COMPARISON: Effectiveness Efficiency Coherence	 + - +	 + - 0
9. **Identification of Beneficial Owner.**	DESCRIPTION: maintain the approach which requires identification of the BO as of a 25% ownership threshold, but clarify what the "25% threshold" refers to, particularly in relation to holding companies, as well as question of indirect ownership.	DESCRIPTION: remove the existing 25% threshold and replace it with a stricter requirement to always find the natural person who owns/controls the company.
	ASSESSMENT: This option would meet the objective of clarification. It would offer flexibility for guidance by ESAs.	ASSESSMENT: This option would target the potential risk (i.e. person who controls the company), with a

	Nonetheless, the concentration on the threshold may not always find the ultimate beneficial owner.	potential positive outcome in terms of effectiveness. However, it would lead to greater expense for obliged entities and to a lack of clarity, unless detailed guidance is prepared. Moreover, the lack of appropriate guidance as to what was expected could lead to a lack of convergence across Member States (as to the interpretation of the person who "controls" a company).
COMPARISON: Effectiveness Efficiency Coherence	 + ++ +	 + 0 -
10. **Home and host supervisory responsibilities for AML**	DESCRIPTION: introduce new rules clarifying that branches and subsidiaries situated in other Member States than the head office apply host state AML rules and reinforce cooperation arrangements between home and host supervisors.	DESCRIPTION: baseline scenario - no change to the current framework, as the Commission has already published a staff working document which clarifies the articulation between the Payment Services Directive and the Third AMLD.
	ASSESSMENT: It would establish a clear legal footing for supervisors. It would in addition increase clarity for businesses and coherence across the EU. On the other hand it could reduce flexibility for Member States.	ASSESSMENT: According to some stakeholders and public authorities the staff working document does not provide sufficient legal certainty for the notion of home host responsibilities. It would therefore not achieve the objective, as it would not provide supervisors and obliged entities with legal certainty.
COMPARISON: Effectiveness Efficiency Coherence	 +++ 0 0	 0 0 0
11. **Sanctions regimes**	DESCRIPTION: introduce a set of minimum principles-based rules to strengthen administrative sanctions, along the lines of the Commission's policy as outlined in its Communication "Reinforcing sanctioning regimes in the financial services sector".	DESCRIPTION: introduce a set of common prescriptive rules (e.g. setting the level of sanctions according to different offences).
	ASSESSMENT: It would enhance compliance by obliged entities and comparability between Member States. It would allow for a more consistent approach across Member States thereby ensuring a greater level playing field and facilitating the business environment.	ASSESSMENT: It would fulfil to a certain extent the objective as it would create a more level playing field, while enhancing coherence across Member States. The Commission's policy outlined in its Communication "Reinforcing sanctioning regimes in the financial

		services sector" already partly advocates such an approach. However, in the field of AML, moving beyond the principles based approach would not allow for flexibility for Member States and it could prove to be difficult in practice to agree on a more detailed and prescriptive approach.
COMPARISON: Effectiveness Efficiency Coherence	 ++ + +	 - - + +
	Policy Options relating to Operational Objective 3 *(Ensure that the rules are risk-focused and adjusted to address new emerging threats, by strengthening and clarifying current requirements).*	
	Preferred Options	**Alternative Options**
12. **Broadening scope to cover gambling**	DESCRIPTION: broaden the scope of the Directive beyond "casinos" to cover the gambling sector, based on a broad definition of gambling. The scope for exemptions from coverage would be limited only to circumstances where there is a very low risk of ML/TF.	DESCRIPTION: adapt the scope to cover gambling activities where there is a proven higher risk.
	ASSESSMENT: This option would achieve our objective in terms of effectiveness, efficiency and coherence. It would enhance effectiveness of the fight against ML/TF and it would be simpler to apply. It would level the playing field within the gambling sector, given the fact that some Member States already apply AML rules across the gambling sector. In contrast, it would entail additional costs to sectors not currently covered by the framework and additional costs to supervise.	ASSESSMENT: This option would enhance the effectiveness of the fight against ML/TF, it would level the playing field with non-obliged gambling sector. At the same time, in terms of efficiency, it would not impose any costs on the gambling businesses which remained outside the scope of the Directive. However, it would be more complex to apply due to the need for identification of higher risk activities and it would entail additional costs to supervise.
COMPARISON: Effectiveness Efficiency Coherence	 ++++ 0 +	 + - - -
13. **Data protection**	DESCRIPTION: introduce new rules in the Directive to clarify the interaction between AML/CFT and data protection requirements, in particular relating to data sharing within groups.	DESCRIPTION: require Member States to clarify interaction between AML/CFT and data protection rules at national level.
	ASSESSMENT: This option would enhance coherence across Member States, would help reduce legal uncertainties	ASSESSMENT: It would help reduce legal uncertainties with which businesses are confronted and

	businesses are confronted with and would bring about cost savings for groups. It would be in line with the new international standards.	therefore enhance their compliance with AML rules. It would moreover ensure compliance with a high level of data protection. Nonetheless, it would not remove incoherence across Member States as a result of differing national interpretations.
COMPARISON: Effectiveness Efficiency Coherence	 +++ 0 +++	 ++ + -
14. **Thresholds for traders in high value goods**	DESCRIPTION: reduction of the scope and CDD thresholds for traders in high value goods from €15,000 to €7,500[70] for cash transactions. CDD measures would need to be applied for cash transactions of €7,500 and above.	DESCRIPTION: reduction of the scope and CDD thresholds to zero for specified obliged entities (e.g. dealers in precious metals and stones, second hand car dealers, etc.).
	ASSESSMENT: It would address risk of use of cash, while bringing the threshold more in line with the common practice in Member States. It would bring more obliged entities into the scope, with potential cost implications.	ASSESSMENT: On the one hand it would ensure firm controls on the use of cash, while a single threshold would promote certainty. Some Member States already apply lower thresholds or indeed even forbid use of cash for certain transactions above certain thresholds (see Table 5). On the other hand, such an approach could drive the use of cash underground, and impact on financial inclusion
COMPARISON: Effectiveness Efficiency Coherence	 +++ 0 +++	 + - +
15. **Cross-border cooperation between FIUs**	DESCRIPTION: introduce new provisions into the Directive regarding FIU powers and cooperation, including an explicit legal basis for the matching of anonymous data between the EU FIUs and clarifying the	DESCRIPTION: establish a single European FIU to receive and analyse and disseminate to the competent authorities disclosures of information from obliged entities operating within

70 The choice of a €7,500 threshold is explained by simply halving the existing threshold. 9 Member States currently apply thresholds below the existing €15,000 stipulated in the Directive, of which 4 Member States apply thresholds below €7,500. The expected impact on traders of a reduction of the threshold would not be to increase costs, but rather to substantially reduce the number of transactions taking place using cash - to the advantage of other payment means (which may carry some additional costs – e.g. fees related to a credit card transaction). The impacts associated with the application of different thresholds (e.g. €10,000, €5,000) have (in the absence of available data) not been assessed, however it is reasonable to assume that they would not reveal significant differences with respect to the likely costs incurred by traders. There would however be different impacts on the number of cash payments, according to the chosen threshold.

	circumstances under which exchange of information can take place .	the EU.
	ASSESSMENT: Introducing new requirements would strengthen FIU powers and cooperation. It would enhance effectiveness of the fight against ML/FT, as well as give legal clarity. However, some difficulties to exchange information may still remain.	ASSESSMENT: This option would enhance effectiveness of the fight against ML/TF; it would also bring about potential advantages in terms of economies of scale and efficiency. However, it would require substantial modifications to Member States' laws permitting cross-border cooperation and information sharing. In addition it could have a negative impact on the agreement of the Member States on the whole package.
COMPARISON: Effectiveness Efficiency Coherence	 +++ 0 +	 + 0 0

VI. ANALYSIS AND QUANTIFICATION OF IMPACTS

VI.1. Compliance costs of the existing framework

While the Third AMLD was not accompanied by an Impact Assessment at the time of the proposal, the cost implications of the current framework have nevertheless been evaluated on an ex post basis. In 2009 an external study[71] by consultants Europe Economics on behalf of the Commission assessed the costs of compliance with a number of Financial Services Action Plan measures (FSAP)[72], including the Third AMLD. The study concentrated on firms from four sectors within the financial services industry in the EU: banks and financial conglomerates, asset managers, investment banks and financial markets.

The study's findings indicated that the cost of compliance with AML requirements was not insignificant and had increased in recent years following the regulatory changes introduced in the EU, notably through the Third AMLD[73]. The focus was on the so-called 'incremental compliance costs' caused by the FSAP measures, rather than on the total costs of activities that contribute to regulatory compliance.

71 Europe Economics: Study on the Cost of Compliance with Selected FSAP Measures, 5 January 2009.

72 The study examined six directives: the Prospectus Directive, the Financial Conglomerates Directive, the Capital Requirements Directive, the Transparency Directive, the Markets in Financial Instruments Directive – MiFID and the AML Directive.

73 However, an important consideration is that the costs of complying with AML measures in a non-harmonised environment would most likely be higher, particularly for cross-border businesses.

The study identified separately cost impacts that were of a one-off nature (i.e. those costs that only have to be incurred once in making the transition, such as IT investment and the re-shaping of business processes) from those that were recurring in nature (on-going costs as a result of regulation). The one-off costs of compliance with the AML Directive for banks, financial conglomerates and investment banks roughly accounted for 10% of all their financial services regulatory costs, while for on-going costs of compliance, the percentage increased to around 13% of all their financial services' regulatory costs.

The main source of AML-related compliance spending was on IT. In terms of one-off costs, this included projects designed to: (i) meet the "Know Your Customer" requirements; (ii) facilitate increased monitoring of suspicious transactions through increased automation of processes; (iii) facilitate PEPs screening; and (iv) assist in risk assessment. In terms of on-going costs, the majority of IT expenditure was linked to access costs to various databases dedicated to the tracking and screening of relevant parties such as PEPs, watch lists etc. While some firms (generally larger banks) viewed automation as the only way to provide the necessary evidence of an audit trail to the regulatory authorities in the event of problems arising (as well as being cost effective by comparison to manual effort), a number of firms had opted to retain significant (or total) human oversight in this area. Training and (for larger banks) recourse to external consultants were also important sources of costs.

VI.2. Measuring Administrative Burden under the existing framework

The study carried out by Europe Economics on the costs of compliance of the Third AMLD contained elements relevant to the measurement of administrative burden in the case of different types of financial institution. The calculations closely reflect those measured under the Standard Cost Model (which breaks down regulation into a range of manageable components that can be measured; information obligations[74], data requirements[75] and administrative activities[76]). The costs measured in the study in large part relate to similar measurable elements (implementation of IT systems, reporting (both internal and external), hiring additional staff, as well as costs relating to understanding legal requirements). To the extent possible, these costs have been calculated to exclude business as usual costs related to information needs which would be necessary without the imposition of AML rules. In the table below, which specifically relates to administrative burdens borne by banks and financial conglomerates, the costs are broken down according to one-off and ongoing costs, and are presented as a percentage of the total compliance costs associated with the Third AMLD. The types and level of costs will differ across business models, however this information is also illustrative of the types of costs facing those entities that will be newly obliged under the enlarged scope of the new proposal.

Table 8 Breakdown of costs associated with administrative burden (banks and financial conglomerates)

One-off costs

74 Information obligations are the obligations arising from regulation to provide information and data to the public sector and / or third parties

75 A data requirement is each element of information that must be provided in complying with an information obligation

76 To provide the information for each data requirement a number of specific administrative activities have to be carried out. Activities may be done internally or be outsourced

Familiarisation with the Directive	3 %
Consultancy fees	11 %
Legal Advice	1 %
Training	22 %
Staff recruitment costs	2 %
Investment in/updating IT	54 %
Project Management	7 %
Other	0 %
Mean incremental cost per bank of measures related to implementation of the Third AMLD	**€ 4,588,000**
Ongoing Costs	
Additional staff	37 %
Internal Reporting	4 %
IT	31 %
External Reporting	5 %
Training	13 %
Audit	10 %
Other	0 %
Mean value of ongoing compliance cost per bank related to the requirements in the Third AMLD	**€ 1,195,000**

Further analysis is provided in Annex IV.

VI.3. Compliance Costs resulting from the changes to the framework

Measuring the compliance costs resulting from the changes to the framework is particularly challenging for a number of reasons:

- In practice, there is no reliable methodology which would allow clear separation of additional costs from business as usual costs (e.g. costs associated with correct customer identification, IT costs relating to the general administration of the system, distinction from periodical IT system upgrades, etc.);
- Precise information from stakeholders has been difficult to obtain, and information from reliable independent sources is very scarce;
- Possibilities to extrapolate across sectors using existing data are limited, as the types of entity, and the cost structures, are so diverse.

Nevertheless, this section has pulled together available information which, although only partial, is intended to illustrate the key cost elements associated with the introduction of a new framework.

The changes to the existing framework will have a number of impacts for obliged entities, such as those identified in the Europe Economics study (the need for new IT investments, staff training, a potential increase in the number of consultations of external data bases - e.g. as a consequence of the broadened requirement to consider also domestic politically exposed persons), an increase in the number of suspicious transaction reports to be filed (e.g. as a result of the obligation to file suspicious transaction reports in any country affected by a suspicious wire transfer). Where the scope is broadened to encompass entities that were hitherto outside the scope of the framework (e.g. in the gambling sector, in those Member States that have not already extended the scope of their AML legislation beyond casinos[77]), there will also be one-off costs linked to investment in new systems. Such one-off costs are expected to be lower in the case of obliged entities who are already applying the AML/CFT rules.

This section is aimed at analysing the administrative costs that could be imposed by introducing a new legal framework; the costs that obliged entities may incur can be classified in different categories: (i) one-off costs (i.e. those costs that only have to be incurred once in making the transition, such as IT investment and the re-shaping of business processes) and; (ii) ongoing compliance costs (i.e. IT expenditure linked – in particular to access costs to various databases dedicated to the tracking and screening of relevant parties such as Politically Exposed Persons, watch lists etc., and additional staff).

The below table summarises the most significant impacts of the proposed revisions to the AML framework and their cost implications, where relevant for existing obliged entities, newly obliged entities, supervisory authorities, national administrations, FIUs as well as, in the case of beneficial ownership information, the costs for all legal entities.

Table 9 Cost/impact implications for various new measures (preferred options)[78]

		One off costs	Ongoing costs
Greater integration of a risk-based approach (relevant to dimensions 2, 3a, 3b and	Obliged entities	**- Potential high impact:** adaptation of existing systems will entail IT and staff training costs, as well as staff costs associated with identification, assessment and mitigation of the entity's own ML /TF risks[79]. For example, in the case of law firms, the cost of putting in place new risk assessment procedures has been estimated by the UK Law Society to	**- Medium impact:** continual training and updating of risk assessments.

77 See Annex IX: Comparison of EU Member States' rules implementing AML rules to casinos and the gambling sector

78 Where information is available, cost quantification is provided on the basis of specific examples. In all cases, impacts are subjectively estimated in terms of "high", "medium" or "low" impacts. In a small number of cases, impacts can be positive – hence each impact is also measured according to its +/- implications.

79 Elements of costs associated with the implementation of the Third AMLC are provided in sections VI.1 and VI.2

		One off costs	Ongoing costs
4 in Table 7)		average £1,200 per larger firm, and £300 per smaller firm[80]. Across the sector in the UK, the total cost is estimated at around £2.5 million.	
	Supervisors	**- Potential high impact:** will need to review ML/TF risk profiles and risk assessments prepared by the supervised entities. There will also need to be coordination at EU level and identification of supranational risk elements.	**- Potential high impact:** They will need to apply a risk-based approach to supervision, based on their understanding of the ML/FT risks present in the country and within the entities they supervise. In the financial sector, until now the supervisory approach (in particular the number of on-site inspections) varies significantly across EU Member States[81]
	National administrations	**- Potential high impact:** A comprehensive national risk assessment needs to be undertaken – an authority needs to be designated to coordinate actions to assess risks and apply resources aimed at mitigating risks.	**- Potential high impact:** The risk assessment needs to be kept up-to-date. Work will be needed to coordinate risk assessments at EU level
Broaden the existing scope (relevant to dimensions 1, 12 and 14 in Table 7).	Existing obliged entities	**- Low impact:** given that some systems are already in place, although new elements (e.g. risk assessments) will still need to be carried out.	**- Low impact**: inclusion of tax crimes as a predicate offence may entail broader monitoring for suspicions of the predicate offence than is currently the case, although this is not expected to impact significantly.
	Newly obliged entities	**- Potential high impact:** e.g. in the gambling sector, newly obliged entities will need to make investments in new systems, staff training, etc. Although the business models differ significantly and cross-sector extrapolation should not be done lightly, experience in the financial sector indicates that one off costs associated with adapting to AML/CFT requirements can account for between 0.16 - 0.29 % of total operating expenses.	**- Potential high impact:** IT expenditure, additional staff recruitment costs, costs linked to access to databases (PEPs, etc.). Experience in the financial sector indicates that on-going compliance costs amounted to 0.05%-0.13% of operating expenses. In the gambling sector, significant business as usual costs (e.g. efforts to counter the risks of fraud and cheating, monitoring the activities of players in order to safeguard the gaming

80 The UK Law Society has provided some estimates of the costs of compliance with respect to putting in place risk assessment procedures:

- With respect to the need to review existing procedures/policies/risk assessment and update them, provide training to relevant staff, including those in the regulated sector as well as the specialist compliance staff and ensure that any system changes are implemented: if it took an MLRO, on a salary of £60,000 pa, one week to review the revised requirements and implement them, without taking into account the training costs/lost fee earning time, the cost incurred would be about £1,200 per firm.
- For smaller firms, the task is likely to be more onerous as their existing risk-based procedures may be less sophisticated and may need more work to ensure they are sufficiently robust. As a supervisor, the Law Society is committing to assisting firms to meet their obligations and is in the process of developing an AML/CFT toolkit to complement our AML/CFT practice note. Such toolkits issued by the Law Society in other areas generally retail for £60 and should be able to be tailored to the firm within a day. Using the same approach as above, the cost incurred would be £240 plus £60 i.e. £300. There are about 8,500 firms of between 1 to 4 partners giving a total cost of about £2.5m for that sector.

81 Source: draft final report by Matrix Insight on the study on the application of the Regulation on information accompanying transfers of funds. For example, in UK, the number of visits undertaken in 2010 to non-bank PSPs specifically related to AML/CFT and the Fund Transfers Regulation (FTR) amounted to 1,964, resulting in 396 warning letters. However this figure is substantially higher than compared to other jurisdictions (for which information was available). In no other case did the number of on-site visits exceed 50.

		One off costs	Ongoing costs
		Only 9 Member States have restricted their frameworks to casinos only (see Annex IX) – in the other cases, parts or all of the gambling sector are already covered, hence the impact in those countries will be less significant. Some impact for traders in goods as a result of reduction of threshold to €7,500 for cash transactions, although it is most probable that rather than incur AML compliance costs, most traders would insist on non-cash means of payment above the threshold. .	activities), already occur, meaning that the incremental ongoing costs of administering additional AML checks may not be that great. The variety of business models in the gambling sector make estimating average costs challenging. By way of example, information provided by the industry[82] on the costs of AML compliance in the case of two casinos in the EU under the existing framework illustrates the significant differences according to the size of the business. In the first example, the total costs of compliance annually amounted to €118,050. In the second example of a larger casino, annual compliance costs amounted to €1,038,400. As AML requirements entail seeking knowledge and understanding of customers, there are likely synergies between existing practices and the new requirements. For traders in goods and services operating above the €7,500 threshold for cash transactions[83], the number of customers who need to be verified for AML purposes is likely to be very low in reality. 6 EU Member States already apply thresholds below €15,000.
	Supervisors	**- Medium impact:** Supervision of entities not hitherto covered will entail additional costs for supervisors and may require more staff as well as systems adjustments – this mainly affects the gambling regulators.	**- Medium impact:** More staff will be needed for supervision of newly obliged entities (mainly in the gambling sector).
	Financial Intelligence Units	**- Low impact:** Systems adjustments may/may not be needed to handle investigations into tax crimes (in some Member States, tax crimes are already covered) and the broader scope of gambling activities.	**- Low impact:** Reception and analysis of additional STRs. Outreach and feedback to newly obliged entities.
Expand definition of PEPs (relevant to dimension 5 in Table 7)	Obliged entities	**- Low impact:** Initial identification of domestic PEPs and PEPs working in international organisations will be necessary	**- Potential high impact:** Additional costs will be needed in order to check PEPs databases, and to periodically review existing domestic PEPs. Increase in administrative costs due to more false positives. By way of example, a query to a private database in the UK costs between £0.15 - £1.00, depending on the profile of the customer. However in the case of e.g. the gambling sector, consultations of such databases are not solely required

82 The European Casino Association

83 E.g. second hand car dealers, dealers in precious metals and stones, auction houses, etc.

		One off costs	Ongoing costs
			with respect to AML compliance, but also may be required for other purposes (e.g. need to check eligibility, age, etc..)
	Supervisors	**- Low impact:** Guidance to obliged entities on how the new rules on PEPs need to be interpreted.	**- Low impact:** Possible additional supervision of risk decisions taken for new categories of PEPs.
	Financial Intelligence Units		**- Low impact:** Reception and analysis of additional STRs as more classes of PEPs are monitored may have resources implications.
Enhance availability of beneficial ownership information (relevant to dimension 6 in Table 7)	Obliged entities	**- Low impact** – no implications for major systems changes.	**+ Potential high positive impact:** Greater assistance in identifying the BO should lead to reduced costs. Information provided by the European Federation of Accountants (FEE) indicates that under the existing framework, CDD checks take on average 0.5-1 hour for "normal" clients, but up to one day, or even two days, in the case of more complex corporate/trust clients. Similar estimates might be applied in the case of the legal profession. Improvements in transparency resulting from an obligation on firms to have information on their beneficial ownership already available would be expected to considerably reduce the time required for CDD checks.
	National administrations	**- Low/medium impact:** Depending on which option is chosen by a Member State, possible cost of setting up a national register.	**- Low/medium impact:** Possible cost of maintaining a national register.
	Firms	**- Potential high impact:** New requirement on firms to hold and make available information on their beneficial owner(s). For individual firms, this requirement would not be expected to entail significant burdens. However given the total number of firms to which this would apply, there could be significant cumulative impacts.	**- Potential high impact:** Need to keep information on BO updated. Firms are better placed to understand their ownership structure than obliged entities – for many (especially smaller) firms this is not expected to amount to substantial additional costs. Costs are likely to be higher in case of firms with more complex and fluid ownership structures.
Enhanced information requirements for electronic transfers (relevant to dimension 7 in Table 7)	Obliged entities	**- Low impact:** Inclusion of beneficiary information is not expected to result in significant additional costs as it is already included in most fund transfers. Concerns have been expressed about potential initial difficulties in the case of PSPs, who operate globally and also in developing countries. In case of slower adaptation in developing countries, it may be necessary to suspend business relationships with PSPs in those countries, leading to potential serious costs[84].	**- Low impact:** Increased costs to be expected due to incomplete information about the beneficiary (payment will be either rejected or more information from the payee's institution requested). However evidence supplied by external consultants responsible for reviewing the FTR suggests that rejection of transfers does not seem to be common practice of PSPs, as issues around missing information tend to be resolved in a different way (e.g. requests for complete information, dialogue with counterparts, etc.).

[84] Information provided by Matrix Insight consultants, in the context of their study on the application of the Regulation on information accompanying transfers of funds

		One off costs	Ongoing costs
	Financial Intelligence Units	**- Low impact in terms of costs.** Law enforcement authorities and FIUs should have a more effective tool to trace terrorist/criminal fund transfers.	**- Low impact:** Possible increase in the number of STRs filed.
Clarify home/host supervisory respons-ibilities (relevant to dimension 10 in Table 7)	Obliged entities	**- Medium impact:** requirements to comply with host state AML rules may entail the need for a local compliance structure/facility.	**- Medium impact:** requirement to file STRs locally will have cost implications (these will vary according to the type of business model) although clarification of supervisory arrangements should facilitate business (greater legal certainty).
	Home Supervisors	**- Low impact:** Need to provide information on obliged entities to host state supervisors. Need to establish appropriate cooperation arrangements with host supervisors.	**+ Low impact:** emphasis on cooperation between home and host supervisors means that some of the tasks normally carried out by the home supervisor may need to be carried out by the host supervisor.
	Host Supervisors	**+ Medium impact:** Will need to put in place arrangements to ensure compliance with local AML/CFT. However such structures should facilitate the job of supervision. They will also need to work closely with home supervisors to establish appropriate cooperation arrangements.	**+ Medium impact:** Supervisors should have the possibility to rationalise AML/CFT compliance supervision through proportionate measures, e.g. local AML compliance structures.
Strengthen and converge national penalty regimes (relevant to dimension 11 in Table 7)	Obliged entities		**- Potential high impact:** Tougher penalty regimes may have cost implications as they are intended to ensure increased attention to full compliance with AML rules.
	Supervisors	**- Medium impact:** Possible legislative changes needed to increase sanctioning powers	**+ Potential high impact:** The ability to sanction firms more heavily for non-compliance should encourage supervisors to exercise increased vigilance to ensure full compliance with AML rules.
Clarify the application of data protection rules (relevant to dimension 13 in Table 7)	Obliged entities	**- Medium impact:** Systems changes and training costs in order to ensure compliance with data protection rules	**+ Potential high impact:** lower costs resulting from greater legal certainty and more efficient rationalisation of data gathering and dissemination within the group.
	Supervisors	**- Medium impact:** Familiarisation with new measures will have staff training implications	
	Financial Intelligence Units	**- Low impact:**	**+ High impact:** Clarification of the rules on exchange of data would increase legal certainty about the conditions under which information on STRs can be shared.
Strengthen the capacity of FIUs to cooperate across borders (relevant to dimension	Financial Intelligence Units	**- Medium impact:** Some systems changes may be necessary to enhance the cooperation capacity of FIUs (e.g. access to national databases)	**- Medium impact:** New powers (e.g. to postpone financial transactions) might imply an increased role for FIUs – implying additional resources. Enhanced cooperation will mean additional resources in order to respond to requests from other FIUs.

		One off costs	Ongoing costs
15 in Table 7)			

VI.4. Impacts of the Framework on Stakeholders

The following table assesses the impacts on the various stakeholders of the proposed changes to the AML/CFT framework, including those not included within its scope, but affected in different ways all the same.

Table 10 Main stakeholders affected by the proposed changes to the AML/CFT

Who is affected?		How?
1. Obliged entities	• Credit and Financial institutions	*Credit and financial institutions have had the most experience in applying AML/CFT rules, and the changes under proposal should not significantly impact their business models. It will be challenging to apply a more risk-based approach, although this element of the new standards has been generally welcomed by the industry. Clarification of data protection rules should facilitate AML/CFT compliance, as should measures to make beneficial ownership more accessible. The requirement under the Fund Transfers Regulation to include beneficiary information is not expected to generate substantial additional impacts, as in most cases fund transfers already incorporate such information. Widening the definition of PEPs will have some impact on these institutions, who will need to assess the risks and apply appropriate measures to additional categories of customers.*
	• Auditors • External accountants • Tax advisors • Notaries • Independent legal professionals (involved in transactions)	*The general scope of application of the Directive will not change with respect to business professionals. On the one hand, application of the risk-based approach could lead to more effective allocation of resources within companies, and the ability to focus on the riskier elements of business might carry advantages for professionals and SMEs working with lower risk clients (the converse is also true – higher risk clients will require more thorough checking and procedures). New rules on PEPs may also require more frequent consultation of external databases.*
	• Trust or company service providers (TCSPs)	*Depending upon the option chosen by Member States for complying with beneficial ownership obligations, TCSPs could be required to hold and maintain information on the beneficial ownership of corporate entities. The implications of this will vary according to the option(s) chosen by Member States.*
	• Real estate agents	*The only change potentially affecting parts of the real estate sector specifically will be an extension of the possibility to allow self-regulatory bodies to monitor and ensure compliance with the AML/CFT rules (Art. 37.4 3AMLD). Otherwise, real estate agents will be impacted in similar ways to other obliged business professionals, as described above.*
	• Casinos/gambling	*Those businesses in the gambling sector which already apply the AML/CFT provisions will be affected in similar ways to*

Who is affected?		How?
		those described above. There will also be a levelling of the playing field with other businesses active in the gambling sector which until now have not been covered by the AML/CFT framework. For those businesses, there will be important adjustments, and investments needed in the form of IT systems and training, as well as new ongoing compliance costs.
	• Other natural/legal persons trading in goods when cash payments <€15,000	*A particular impact will be the reduction of the €15,000 scope threshold to €7,500, which may make an additional number of entities subject to the requirements of the Directive, but will most likely rather encourage traders (e.g. precious metal dealers, second hand car dealers, auction houses) to accept non-cash payments..*
2. Public authorities	• Regulators • Supervisors	*The strengthening of the risk-based approach will require national risk assessments to be compiled. Guidance will need to be provided to obliged entities on how to apply the rules, and supervisors will also need to develop risk-sensitive supervision – which should allow them to more effectively target their resources to areas of greater risk. There will also be a role for the AMLC at European level to contribute to supranational elements of risk and threat assessments for obliged entities in their sectors.*
	• Financial Intelligence Units • Law enforcement	*The strengthening of cooperation arrangements, which is not expected to impose significant additional costs, as well as the clarification of data protection rules, should benefit the work of FIUs from an effectiveness perspective. Law enforcement should benefit from the overall strengthening of the AML/CFT framework, which should result in greater detectability of criminality (improved detectability of electronic fund transfers, PEPs, BOs,..). At EU level, both the FIU platform as well as Europol will be expected to contribute to supranational risk and threat assessments.*
	• National registries	*Depending on which option Member States choose for making beneficial ownership information available, the setting up and maintaining of public registries is something that might impose additional costs.*
3. Customers	Customers of the obliged entities (banks, financial institutions, auditors, etc.)	*No major impacts are expected for customers of obliged entities (fundamental rights issues are separately assessed under section VII.1) resulting from changes to the existing framework. However the extent to which AML rules in general may/may not contribute to financial exclusion (e.g. due to refusal by some banks to open accounts for customers on the grounds of money laundering concerns) remains an important issue. An analysis of the Third AMLD by Commission services has concluded that the Directive in itself does not create any barriers to opening accounts. In particular, the current AML provisions do not require a person who wishes to open a bank account to produce an ID card or passport. It can therefore be concluded that it is rather financial institution's own internal processes or bank staffs' perhaps overly cautious application of anti-money laundering rules which may be creating these "false barriers". The introduction of a risk-based approach and its application to customer due diligence procedures may in fact have a positive impact, potentially limiting any refusals to open accounts to genuine cases of ML/TF risk. This issue is more*

Who is affected?		How?
		broadly addressed in another initiative currently under consideration by the Commission on payment accounts. *In the case of the gambling sector, customers of establishments newly covered by the AML/CFT rules will be required to provide proof of identity above a threshold of €2,000.*
4. Business	Business community in general	*Depending on which option Member States choose for making beneficial ownership information available, the potential requirement on companies to hold information on their shareholders and their beneficial owners will have impacts on the business community. The burden will be partly shifted from the obliged entities to the corporate customers of the obliged entities, who are better placed to provide information about their ownership.* *No other major impacts from the changed rules are to be expected, either on larger businesses or for SMEs.*
5. Perpetrators	Criminals, including terrorists and corrupt PEPs	*Criminals, terrorists and corrupt PEPs should find it harder to launder or transfer funds, as their activities will be subject to more effective monitoring by obliged entities, FIUs and law enforcement.*
6. EU Victims	EU Society/citizens	*Strengthening the AML/CFT framework should have societal benefits – protecting society against terrorism and criminal abuse of the financial system.*
7. Non EU Victims	Society/citizens/governments in third countries	*The adoption of international standards should mean that high AML/CFT standards are achieved across the globe. Strengthening the EU system should ensure that the proceeds of corruption, which drain away wealth and resources from third countries, and the proceeds from all other predicate offences are less easily processed through the EU financial system.*

VII. ANALYSIS OF OTHER IMPACTS

VII.1. Impact on fundamental rights

The Commission's proposal, which has to respect the Charter of Fundamental Rights of the European Union ('the Charter')[85], should strengthen fundamental rights laid down in the Charter. The proposal will help to protect the fundamental right to life (Article 2 of the Charter) which is threatened by criminal activities and terrorism. The Charter also recognizes as a fundamental right the protection of private life and personal data (Articles 7 and 8 of the Charter). Article 52 of the Charter[86] recognizes that some limitations to fundamental rights may be laid down by law if proportionate and necessary, for example to protect fundamental rights and liberties of other people [87]. Finally, the proposal will have no impact on the right to

85 http://www.europarl.europa.eu/charter/pdf/text_en.pdf

86 CJEU, judgment of 9.11.2010 in joined cases C-92/09 and 93/09, Schecke.

87 The principles of necessity and proportionality are also required by Article 8 of the Charter and Article 16 of the Treaty on the

an effective remedy and to a fair trial (Article 47 of the Charter), as no changes to the current provisions are proposed in this respect . Although legal professions regularly express concerns that this right and their obligation of professional secrecy would be violated by AML/CFT obligations to report suspicious transactions, the European Court of Justice[88] has ruled that since reporting obligations only apply to activities of a financial or real estate nature and do not apply in the context of judicial proceedings, they fall outside the scope of the right of a fair trial.

AML/CFT legislation requires obliged entities to know their customers – as well as certain other persons who are not always their customers (e.g. beneficial owners) – and to assess their associated ML/TF risks. For that purpose, obliged entities need to collect, process and record personal data, and sometimes to share such data with public authorities (such as FIUs) or with private entities within the same group. These requirements have implications for such persons with respect to their rights regarding respect of private life and protection of personal data while having an overall security impact (general interest).

The proposal should also reinforce fundamental rights by bringing clarification on how institutions need to apply AML/CFT requirements in a way which is compatible with a high level of protection of data, in comparison to the current situation where legal uncertainties can lead to inefficient outcomes (i.e. as regards their degree of protection of data). As an example, by specifying the conditions under which data can be retained, protection of data subjects will be strengthened.

The different options considered in this impact assessment[89] and aimed at clarifying data protection rules will not have identical impacts on fundamental rights. Under Dimension13 in Table 7, the option which aims to clarify the interaction of data protection and AML/CFT rules at EU level would be the only option which would ensure the same level of protection for all citizens of the EU, whereas clarification at Member State level would leave room for divergent interpretations, incoherence across Member States and would thus not place all EU citizens on an equal footing.

Some of the proposed measures considered in this impact assessment may involve a degree of limitation to the right of respect for private life and data protection, such as the proposal to enhance availability of information on shareholders, beneficial ownership and nominees (Dimension 6). The proposal would limit the possibility for some persons to make use of corporate vehicles where beneficial ownership information is not always immediately apparent. However, this limitation would be formulated in a clear and proportionate manner (these persons would need to know in advance that information on them could be accessed, as this possibility would be foreseen in the law) and the Commission considers it necessary in order to achieve the objectives of enhancing the effectiveness of the fight against ML/FT and complying with the new international Recommendations. Currently there is a gap in the AML legislation, as institutions are required to know their customers and understand the nature of their business, but have difficulties to access information on them as such information is not publicly available. This limitation would also be proportionate to the aim and preserve the essence of the right. It would still be possible to use legal entities and arrangements such as

---

Functioning of the European Union)

88 ECJ C305/05, Ordre des barreaux francophones et germanophones et al. V Conseil des Ministres, Para 33, Judgment of the Court, 26 June 2007.

89 See Option 13 in Annex III

nominee companies or trusts, but information on them would be more accessible. The different options considered with respect to availability of beneficial ownership information would not have identical impacts on fundamental rights. If availability of information were limited to competent authorities and obliged entities, the limitation would be strictly proportionate to what is necessary to achieve the objective of helping obliged entities to know their customers. If information were to be made available to all citizens though a public register, this would constitute a more substantial limitation to the privacy right, but would allow the attainment of other objectives, such as helping other entities not covered by the directive in their fight against ML/TF (e.g NGOs) or fighting tax evasion.

Despite the limitations, requiring enhanced availability of information on shareholders, beneficial owners and nominees would also strengthen privacy and data protection rights, as the information obtained by covered institutions would come directly from the legal persons itself, rather than from potentially less trustworthy sources.

VII.2. Impacts on Small and Medium-Sized Enterprises (SMEs)

The changes to the framework are expected to impact SMEs from two different perspectives:

- ***SMEs which are gatekeepers under the AML framework will be affected by the proposed changes***: the most significant change is likely to be the enhancement of the risk-based approach, intended to lead to more effective allocation of resources within companies. SMEs operating under the framework (e.g. small offices of lawyers or accountants, independent professionals, and smaller financial institutions, etc.) have frequently complained that AML/CFT rules have been designed with larger financial institutions in mind, and that they do not have adequate resources to conduct the same level of control as would, for example, a large multi-national bank. The enhanced use of the RBA should allow focus on the riskier elements of business, and for those involved in businesses where ML/TF risks can be proven to be lower, the compliance burden with AML rules should be lighter than for those businesses working with higher risk clients (where more thorough checking and monitoring may be required). In some cases, professional organisations can also play an important role to ease the burden of compliance, through the provision of guidance, organization of training courses, submitting law clarification notes, answering doubts in the application of the legislation, etc.[90]There can be significant cost advantages to be gained for SMEs from such approaches[91]. There will also be impacts stemming from, on the one hand, new rules on PEPs, which may require more frequent consultation of external databases (however the costs associated with such checks should not be exaggerated – in the UK a query to a private database costs between £0.15 - £1.00, depending on the profile of the customer), and on the other hand, from the enhanced transparency of beneficial

---

90 Based on the survey conducted by the Deloitte study, this is the case for a number of national professional associations (notaries, bar associations, etc.). For example, in the case of Spanish notaries a centralised unit has been set up by the General Council of Notaries aimed at preventing and combating ML-FT by integrating and compiling information on transactions performed before all notaries and automating treatment of information (red flags, patterns, etc.).

91 For example in the case of the UK Law Society, which acts as a self-regulatory body, assistance provided to firms to meet their obligations. They are in the process of developing an AML/CFT toolkit to complement their AML/CFT practice note. Such toolkits issued by the Law Society in other areas generally retail for £60 and should be able to be tailored to the firm within a day. Using the same approach as above, the cost incurred would be £240 plus £60 i.e. £300. There are about 8,500 firms of between 1 to 4 partners giving a total cost of about £2.5m for that sector.

ownership information which should make the job of checking on beneficial ownership of clients easier. Traders in high value goods (e.g. jewellers, second hand car dealers, auction houses, etc.) are likely to be affected by the reduction of the threshold above which they become subject to the AML framework. Such persons will need to make a choice on whether to continue to accept cash above the lowered €7,500 threshold and thus perform customer due diligence checks, or whether to decline such cash transactions and request settlement by other means of payment. As compliance with AML rules requires knowledge of the law, staff training and access to AML-related information and data-bases, it is most probable that the large majority of SME's faced with such choices would opt for the latter option.

- ***SMEs which are not subject to AML requirements, but which will be affected by the proposed changes***: the controls and restrictions which result from the existing preventative framework protect businesses from the risks and harmful effects associated with money laundering and terrorist financing. The most significant change affecting the broader business community will be the introduction of rules on enhancing the availability of beneficial ownership information. The requirement on companies to hold information on their beneficial owners will shift some of the burden from the obliged entities onto their customers, who are better placed to provide information about their ownership. The cost impact for individual firms is not expected to be great, however with an estimated 23 million SMEs in the EU, the cumulative impacts of this measure risk to be rather significant. No major other impacts from the changed rules are to be expected with respect to SMEs.

VII.3. Environmental impacts

The environmental impact of the proposed changes is likely to be minimal.

VII.4. International aspects

VII.4.1. International Standards

The FATF is recognised as the global standard-setter for AML and CFT. Its recently revised 40 Recommendations set out the international framework that over 180 countries globally (through a network of regional bodies) seek to implement. They form the basis for a co-ordinated response to potential threats to the integrity of the financial system and help ensure a level playing field. The Recommendations set out the measures that countries should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and other businesses and professions; measures to ensure transparency on the ownership of legal persons and arrangements; the establishment of competent authorities with appropriate functions, and powers and mechanism for cooperation; and arrangements to cooperate with other countries.

The FATF evaluates the progress of its members in implementing necessary measures and sets remedial action if it deemed appropriate. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

As a founder Member of the FATF, the European Commission participated in the process of revising the FATF Recommendations and has fully endorsed the revisions. Given that all EU

Member States will be subject to mutual evaluations conducted by either the FATF (of which 15 Member States are members) or Moneyval (a FATF-style regional body of which 12 Member States are members), it is appropriate that changes to the Third AMLD be consistent with the new international standards.

VII.4.2. Third Country Equivalence

The EU's Third Country Equivalence process involves an assessment of countries that are deemed to have AML/CFT systems that are "equivalent" to those set out in the Third AML Directive. Countries that are deemed to have "equivalent" systems are named in a list drawn up by representatives of Member States. The grounds for inclusion in the list are set out in the "Common Understanding" drawn up by representatives from Member States. Under the Third AMLD equivalent status gave the possibility for obliged entities in EU Member States to apply reduced measures (for example, simplified customer due diligence measures) in respect of financial institutions from equivalent third countries. It appears that some third countries saw inclusion on the list as a form of unofficial endorsement of the soundness of their AML/CFT systems from the Member States. The move towards a more risk-sensitive system, whilst maintaining some version of a list as an evidential factor of lower geographical risk will still allow comparison of the quality of third country regimes with the AML Directive and could make business with institutions in third countries easier (for example, by applying simplified customer due diligence measures).

VII.4.3. Competitiveness of EU

Although tougher AML/CFT measures will result in some cost burden for obliged persons and entities, the EU should aim to have AML/CFT systems that are robust and that protect the integrity of the financial system within the single market. This should increase the attractiveness of conducting legitimate business in the single market area and maintain confidence in the financial system by those that seek to use it for legitimate purposes.

VIII. OVERALL IMPACTS OF THE PACKAGE

VIII.1. Impacts of the preferred policy options

The preferred policy options outlined in this impact assessment are intended to address the problems as outlined in the problem definition, i.e.:

- Adaptation of the framework in order to adhere to recently revised international AML/CFT standards;
- Clarification of the rules so as to ensure consistent application throughout the EU, but in a way which ensures an appropriate degree of consistency;
- Ensuring that the rules appropriately address existing and newly emerging threats.

While the negative implications of not having in place such systems are explored in various parts of this impact assessment, it is impossible to provide an accurate quantitative estimate of

the **benefits** of having in place up-to-date, internationally compliant rules which are coherent across the Internal Market. The World Bank describes the benefits as follows: "*..an effective framework for anti-money laundering (AML) and combating the financing of terrorism (CFT) have important benefits, both domestically and internationally, for a country. These benefits include lower levels of crime and corruption, enhanced stability of financial institutions and markets, positive impacts on economic development and reputation in the world community, enhanced risk management techniques for the country's financial institutions, and increased market integrity*."[92]

The adaptation of the framework to stricter international standards, coupled with the additional changes which are proposed as a result of the Commission's own review process are expected to represent a substantial strengthening of the overall framework. The envisaged changes should mean that:

- a broader scope will address additional areas of risk,
- cross-border compliance should be strengthened
- greater coherence between national rules achieved,
- greater effectiveness should result from more targeted and risk-sensitive rules.

In particular, the risk-based approach is not intended to lead to any lessening of standards, but on the contrary it calls for increased vigilance and its application should allow for the most significant AML/CFT risks to be more effectively targeted.

The FATF is increasingly focussing on the effectiveness of AML rules, as opposed to simple compliance. New ways to evaluate the national implementation of standards are currently being developed, which should mean that there will be increased onus on competent authorities to demonstrate that their systems are really working and keeping money launderers and terrorists out of the system.

The preceding sections have described the impacts the proposed measures are expected to have from a variety of different perspectives.

In terms of **cost impacts**, it is clear that the implications will be very different according to the situation of various stakeholders. The most significant cost factors associated with AML compliance are those connected with initial one-off costs associated with the introduction of new systems, training, consultancy, etc. On the basis of a previous Commission study[93], it is already clear that how high those costs are likely to be will very much depend on the type of strategy adopted to ensure compliance (e.g. focus on automated processes, as opposed to manual processes). It will also depend on the degree of AML/CFT risk associated with the nature of each business. Experience in the financial sector suggests that one-off AML compliance costs can amount to as much as 10% of all their regulatory compliance costs, although caution is required when attempting to extrapolate such data to other obliged entities

92 Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism Second Edition and Supplement on Special Recommendation IX, The World Bank/IMF, 2006.

93 Europe Economics: Study on the Cost of Compliance with Selected FSAP Measures, 5 January 2009.

operating very diverse business models. It is not expected that existing obliged entities will be unduly impacted by the envisaged changes, as they have already made systems investments which should be relatively easily adapted without the need for heavy new investments. The same cannot however be concluded with respect to entities who were hitherto outside the scope of the AML framework but who will need in future to apply AML/CFT rules. This is notably the case in the gambling sector, where in a number of Member States only "traditional" casinos are currently within the scope of national rules[94].

In terms of **impacts on Member States' AML regimes**, the fact that the international standards have been applied and evaluated in all Member States, coupled with the fact that all EU Member States have fully implemented existing EU rules, suggests that the impact of introducing a revised set of internationally agreed rules via the Commission's proposals should not unduly advantage or disadvantage particular Member States. The quantity and variety of changes will have different implications for the modification of existing legal frameworks at national level. Those frameworks have been conceived to function in different broader legal environments, and therefore the specific impacts in Member States are likely to differ accordingly. Some examples of different Member State approaches have been provided in this impact assessment (e.g. see Box 5 on the different approaches to the calculation of the 25% beneficial ownership threshold, Table 5 on transactions for cash thresholds, Annex VIII comparing EU MS' sanctions and penalties, Annex IX on EU MS' approaches to the regulation of the gambling sector).

In terms of **other impacts**, consideration has been given to how the envisaged measures would affect:

- Stakeholders – both those falling under the scope of the existing framework, and other stakeholders affected by the changed rules.

- Fundamental rights, where it is particularly important to ensure an appropriate balance between effectiveness of AML/CFT measures and the respect to data protection and privacy.

- SMEs, where a distinction is drawn between the impacts on SME's which fall under the scope of the AML/CFT framework, and the impacts on SME's in general.

- The environment – where no significant impacts are foreseen.

- The international dimension, where in particular the current approach towards recognition of third country equivalence needs to be adapted to the risk based approach, which should consequently mean that in future geographical location will be just one factor in a broader assessment of ML/TF risks.

In conclusion, the Commission considers that the proposed rule changes are proportionate to the objectives. By ensuring a tailored and flexible approach, Member States should not be constrained from adopting measures and taking actions as necessary to counter important threats they may confront at national level. The inclusion of processes at EU level to ensure greater coordination and the development of supranational approaches, together with further

94 This is further explored in Annexes V.7 and IX.

harmonisation in specific areas should ensure that EU objectives are also met. Although ensuring an effective AML/CFT system entails considerable costs for obliged entities (these costs have been analysed in Annex IV), the Commission considers that the (much harder to quantify) benefits associated with preventing money laundering and terrorist financing will continue to outweigh the costs, also the new costs arising from the changes to the framework.

VIII.2. Coherence with other EU initiatives

The proposed adaptation to the AML/CFT framework is fully coherent with EU policies in other areas, in particular:

- The **Stockholm Programme**[95], which aims at achieving an open and secure Europe serving and protecting citizens, calls on Member States and the Commission to further develop information exchange between the FIUs, in the fight against money laundering.

- The EU's **Internal Security Strategy**[96] identifies the most urgent challenges to EU security in the years to come and proposes five strategic objectives and specific actions for 2011-2014 to help make the EU more secure. This includes tackling money laundering and preventing terrorism. The need to update the EU AML/CFT framework with a view to enhancing the transparency of legal persons and legal arrangements has been specifically recognised.

- In March 2012, the European Commission adopted a **proposal on the freezing and confiscation of proceeds of crime in the European Union**[97] which seeks to ensure that Member States have in place an efficient system to freeze, manage and confiscate criminal assets, backed by the necessary institutional setup, financial and human resources.

- With respect to **data protection**, the envisaged clarifications to the Third AMLD are fully in line with the approach set out in the Commission's recent data protection proposals[98]. The Commission's AML proposals will strengthen protection of personal data, by limiting the length of time and stipulating the conditions data can be retained by obliged entities, and will clarify the conditions under which transfers to third countries may take place.

- With respect to **sanctions**, the proposal to introduce a set of minimum principles-based rules to strengthen administrative sanctions is fully in line with the

---

95 Official Journal of the European Union, C 115/1, 4.5.2010.

96 Commission Communication: "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM (2010)673 final.

97 Proposal for a Directive on the freezing and confiscation of proceeds of crime in the European Union, COM(2012) 85 final

98 See the Commission's data protection proposals (COM(2012) 11 final) and (COM(2012) 10 final). http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Commission's policy as outlined in its Communication "Reinforcing sanctioning regimes in the financial services sector"[99].

- With respect to **financial inclusion**, the fact that applying an overly cautious approach to AML/CFT safeguards might have the unintended consequence of excluding legitimate businesses and consumers from the financial system has been recognised. Work has been carried out on this issue at international level[100] to provide guidance to provide support countries and their financial institutions in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. At EU level, the issue of financial inclusion is currently under consideration as part of the work on a Bank Accounts package.

IX. MONITORING AND EVALUATION

The Commission is the guardian of the Treaty and will therefore need to monitor how Member States have implemented the changes to the Third AMLD and the FTR. Where appropriate and on request, the Commission services will offer assistance to Member States, throughout the implementation period, for the implementation of the legislative changes in the form of transposition workshops with all the Member States or bilateral meetings. Wherever necessary, the Commission will follow the procedure set out in Article 258 of the Treaty in case any Member State fails to respect its duties concerning the implementation and application of Community Law.

The Commission will work with the joint Committee of the European Supervisory Authorities on AML (AMLC), which in particular produces reports on the implementation of the third AML Directive in some specific areas[101] in order to monitor the application of the new legislative framework. The Committee on the Prevention of Money Laundering and Terrorist Financing (CPMLTF), could also serve as a forum for sharing information on application issues. The Commission services may also use the findings of studies carried out by stakeholders or Member States as well as any feedback from meetings with private stakeholders. Consideration will also be given to commissioning an external study as appropriate[102].

Monitoring of the application of the AML Directive will also take place indirectly through the mutual evaluation processes of the FATF (15 EU Member States are members of this body) as well as Moneyval (the other 12 Member States are members of this body). This peer review

---

99 Reinforcing sanctioning regimes in the financial services sector (COM(2010) 716 final)

100 See "Anti-money laundering and terrorist financing measures and Financial Inclusion", FATF, June 2011

101 See two AMLC reports of 11 April 2012 on the implementation of the third AML Directive. The "Report on the legal, regulatory and supervisory implementation across EU Member States in relation to the Beneficial Owners Customer Due Diligence requirements" and the "Report on the legal and regulatory provisions and supervisory expectations across EU Member States of Simplified Due Diligence requirements where the customers are credit and financial institutions" provided an overview of the legal and supervision framework.

102 Such a study was commissioned in order to assess the application of the current Directive : Final Study on the Application of the Anti-Money Laundering Directive, Deloitte, December 2010

process[103] is an essential and rigorous process to ensure that Member States comply, both in law and in practice, with FATF international standards, from which most of the requirements of the AML Directive are derived. Evaluations take place around every 5-7 years for each country and can be complemented by follow-up reports, usually every 2 years (or more frequently if the deficiencies identified require it). The FATF is placing increased emphasis on the assessment of *effectiveness* of measures, as opposed to compliant legal frameworks. The mutual evaluations concerning individual EU Member States will represent an important element for the Commission's own evaluation of the effectiveness of the legal framework.

As these monitoring options would make use of the existing European or International structures and would not require the setting up of a new instrument, they would entail limited cost at EU level.

As regards progress indicators for the key objectives, good ratings in FATF or Moneyval reports on EU Member States would be indicators of the consistency of the EU approach with international standards and of the preservation of the EU financial system's reputation. The number of suspicious transaction reports, investigations, prosecutions or sentences in the different Member States, compared to those of the previous years, can also constitute a starting point to measure progress in effectiveness of the system against ML/FT[104].

Efforts to monitor effectiveness through the compilation of data at EU level have been made by the Commission, and are described in Annex VII.

Reports produced by the AMLC can also be excellent indicators of the state of coherence of AML legislation and supervisory implementation across Member States in some specific areas[105].

An ex-post evaluation of the application of the revised Directive should take place after the entry into force of the legislative measure in the form of a Commission report to the Council and the European Parliament[106].

---

103 Further explained in section III.4.1

104 These statistical indicators need to be treated with caution as they can also mean an increase in criminal activity or increased resources within the police, judicial or supervisory bodies.

105 The two AMLC reports of 11 April 2012 above-mentioned sought to identify differences in the implementation of the Directive.

106 It will be important to set an appropriate timeframe for the production of such a report, as the period of 4 years following the adoption of the Third AMLD to evaluate the application of the Directive proved to be too short to obtain qualitative and quantitative information about the impact of the Directive in all areas concerned

X. ANNEXES

ANNEX I: GLOSSARY

Anti-Money Laundering Committee (AMLC)	*The Joint Committee of the European Supervisory Authorities´ Sub Committee on Anti-Money Laundering (AML Committee, AMLC) assists the European Supervisory Authorities in a supervisory capacity, to ensure a consistent implementation of the EU law.*
Article 29 Working Party on Data Protection	*The Article 29 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.*
Beneficial Owner	*Article 3(6) of the Third AMLD defines "beneficial owner" as the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted.*
Committee for the Prevention of Money Laundering and Terrorist Financing (CPMLTF)	*Established by Article 41 of the Third AMLD, the role of the CPMLTF, made up of designated Member States representatives as well as a number of observers, is to assist the Commission in the development of AML/CFT policy.*
Customer Due Diligence (CDD)	*Customer Due Diligence is described in Chapter II of the third AMLD. The "regular" level of CDD imposes a duty on the obliged entity to identify and verify their customers and customers' beneficial owners, to understand the purpose and nature of the business relationship as well as to conduct ongoing monitoring.*
Deloitte study	*A Study on the Application of the Anti-Money Laundering Directive carried out on behalf of the European Commission (DG Internal Market and Services):* *http://ec.europa.eu/internal_market/company/docs/financial-crime/20110124_study_amld_en.pdf*
Designated Non Financial Businesses and Professions (DNFBPs)	*Those entities which are not credit or financial institutions but which fall under the scope of the Third AMLD, i.e.:* • *Auditors* • *External accountants* • *Tax advisors* • *Notaries and Independent legal professionals (involved in transactions)*

	• *Trust or company service providers* • *Real estate agents* • *Casinos* • *Other natural/legal persons trading in goods when cash payments <€15,000*
Egmont Group	*The Egmont Group of Financial Intelligence Units is an informal international gathering of financial intelligence units (FIUs). The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field.*
Enhanced Due Diligence (EDD)	*In the case of EDD, the obliged entity must take a number of prescribed further customer due diligence steps, albeit on a risk-sensitive basis.*
European Supervisory Authorities (ESAs)	• *European Securities and Markets Authority (ESMA)* • *European Banking Authority (EBA)* • *European Insurance and Occupational Pensions Authority (EIOPA).* *Set up in January 2011, the ESAs are tasked with financial stability and strengthening and enhancing the EU supervisory framework.* *Jointly they are responsible for the Anti-Money Laundering Committee (see separate explanation)*
FATF fourth round evaluation process	*The FATF conducts evaluations of its members, and completed the third round of these mutual evaluations in 2011. The fourth round is expected to commence in 2013.*
Financial Action Task Force (FATF)	*An inter-governmental body established in 1989 by the Ministers of its Member jurisdictions and organisations. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.*
Financial Intelligence Unit (FIU)	*Article 21 of the Third AMLD requires the establishment of an FIU which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing.*

FIU Platform	*The "EU Financial Intelligence Units' Platform" was set up in 2006 by the European Commission. It gathers Financial Intelligence Units from the Member States. Its main purpose is to facilitate cooperation among the FIUs.*
Internal Security Strategy	*The EU's Internal Security Strategy identifies the most urgent challenges to EU security in the years to come and proposes five strategic objectives and specific actions for 2011-2014 to help make the EU more secure. This includes tackling money laundering and preventing terrorism.*
Legal arrangements	*According to the FATF definition, legal arrangements refer to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.*
Legal persons	*Any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, Anstalt, partnerships, or associations and other relevant similar activities.*
Money Laundering (ML)	*Money laundering is defined in the Third AMLD as follows:* *The following conduct, when committed intentionally, shall be regarded as money laundering:* *(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;* *(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;* *(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;* *(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.*

Moneyval	*Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Moneyval currently comprises 30 members which are subject to its evaluation processes and procedures, including the 12 EU Member States which are not members of FATF. The aim of Moneyval is to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields.*
Obliged entities and persons	*Article 2 of the Third AMLD imposes obligations on financial institutions, auditors, external accountants, tax advisors, notaries and other legal professionals (when participating in any financial or real estate transaction), trust or company service providers, real estate agents and casinos. There is also an obligation on other natural or legal persons trading in goods where payment is made in cash equal to or above €15,000.*
Payment Service Provider (PSP)	*As defined in Art 4(9) of Directive 2007/64/EC (the "Payment Services Directive"), i.e. credit institutions, E-Money institutions, post office giro institutions providing payment services, payment institutions, European Central Banks and national Central Banks when not acting in their capacity as monetary or other public authorities, Member States or their regional or local authorities when not acting in their capacity as public authorities.*
Politically Exposed Person (PEP)	*The Third AMLD defines "politically exposed persons" as natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.*
Predicate offence	*Are serious crimes as described in Art. 3(5) of the Third AMLD. The listed categories of crimes are those for which transformation of the proceeds are considered to give rise to money laundering.*
Risk Based Approach (RBA)	*Under the revised FATF recommendations, the risk-based approach allows countries and obliged entities and persons to adopt a more flexible set of measures in order to comply with certain Recommendations. This helps them to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.*
Simplified Due Diligence (SDD)	*SDD permits obliged entities to perform reduced customer due diligence measures for certain types of customer or*

	business.
Suspicious Transaction Reports (STRs)	*A disclosure made to a Financial Intelligence Unit (FIU) by an obliged entity or competent authority having an obligation to disclose based on the suspicion or reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted.*
Terrorist Financing (TF)	*Terrorist financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism as amended by Council Framework Decision 2008/919/JHA.*
Trust and Company Service Providers (TCSPs)	*As defined in Art. 3(7) of the Third AMLD:* *"Any natural or legal person which by way of business provides any of the following services to third parties:* *(a) forming companies or other legal persons;* *(b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;* *(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;* *(d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;* *(e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards;"*

ANNEX II: THE DEVELOPMENT OF EU AND INTERNATIONAL POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

At international level, the FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism. The FATF Recommendations were first issued in 1990, and revised in 1996, 2001, 2003 and most recently in 2012, after an extensive process involving experts from members, to ensure that they remain up to date and relevant.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures worldwide. The FATF has completed the third round of mutual evaluations of its members, and will commence the fourth round of mutual evaluations at the end of 2013. The results of these assessments are made public and any short-comings identified in the reports are subject to a rigorous follow-up process.

The G20 has recognised and endorsed the revision of the FATF Recommendations and the work of the FATF.

In the EU, there has been a progressive introduction of rules to establish a preventative framework designed to protect the financial system.

The first elements of the EU Anti-Money Laundering framework were put in place through the adoption of Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. It required Member States to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities. The financial sector has progressively implemented AML regimes, and now files by far the largest number of suspicious transaction reports to Financial Intelligence Units (see Table 2 in section III.3.2).

Over the years, the rules have been reinforced.

The Second Anti Money Laundering Directive (2001/97/EC):

- Clarified to which national authorities suspicious transaction reports from foreign branches of credit and financial institutions should be sent;

- Clarified the scope of obliged entities by confirming the inclusion of bureaux de change, money transmitters and the activities of investment firms;

- Expanded the scope of predicate offences to bring it in line with the 1996 FATF 40 recommendations;

- Extended the Directive's obligations concerning customer identification, record keeping and the reporting of suspicious transactions to notaries and independent legal professionals when participating in financial or corporate transactions, whilst allowing

bar associations or the self regulatory bodies to receive reports for possible onward transmission to authorities responsible for combating money laundering.

The Third Anti Money Laundering Directive (2005/60/EC) updated the EU framework in light of the expanded FATF standards, which had been revised in 2003. The new provisions:

- Brought the definition of serious crime into line with the definition of serious crime in Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime.

- Extended the preventive measures to the collection of money or property for terrorist purposes;

- Introduced more specific and detailed provisions relating to the identification of the customer and of any beneficial owner and the verification of their identity;

- Clarified that the obligations from the Directive also applied to activities performed on the Internet;

- Extended the scope of the Directive to cover life insurance intermediaries and trust and company service providers

In addition to these developments, the AML/CFT framework is completed by a number of EU instruments:

- **Directive 2006/70/EC (the "implementing Directive")** lays down implementing measures for Directive 2005/60/EC as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

- **Regulation 1781/2006** on information on the payer accompanying transfers of funds: the Regulation requires information on the payer to accompany transfers of funds, with the objective of ensuring prevention, investigation and detection of money laundering and terrorist financing. The Regulation covers all types of funds transfers carried out by electronic means in any currency, from a payer to a payee, which are sent or received by a Payment Service Provider (PSP) established in the EU (Art. 3.1). This is in order to make it easier for law enforcement authorities to track funds transferred electronically by terrorists and criminals.

- **Regulation 1889/2005** on controls of cash entering or leaving the Community places an obligation on any natural person entering or leaving the EU and carrying cash of a value of €10,000 or more to declare that sum to the competent authorities. The regulation only covers currency and excludes gold or precious metals. In the event of failure to comply with the obligation to declare, cash may be detained by administrative decision in accordance with national legislation.

- **Council Decision 2000/642/JHA** introduces arrangements to facilitate the cooperation of exchanging information between FIUs in the Member States. The Decision seeks to

address the difficulties in communication and exchange of information among FIUs that result from existing different legal status (administrative, judicial or law enforcement based) and providing for direct communication between them. The Decision reflects the standards and principles established by the Egmont Group[107] as well as the recommendations of the FATF.

- **Council Framework Decision 2001/500/JHA** seeks to implement concrete steps on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime. Member States are also required to take necessary steps to ensure that all requests from other Member States, related to asset identification, tracing, freezing or seizing and confiscation, are processed with the same priority given to domestic proceedings.[108]

- **Council Framework Decision 2002/475/JHA** of 13 June 2001 on combating terrorism which urges EU Member States to align their legislation and setting out minimum rules on terrorist offences. After defining such terrorist offences, the framework decision lays down the penalties that EU countries must incorporate in their national legislation.

107 The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field

108 In March 2012, the European Commission took steps to update this framework by adopting a proposal on the freezing and confiscation of proceeds of crime in the European Union. The proposal seeks to ensure that Member States have in place an efficient system to freeze, manage and confiscate criminal assets, backed by the necessary institutional setup, financial and human resources (see Proposal for a Directive on the freezing and confiscation of proceeds of crime in the European Union, COM(2012) 85 final).

ANNEX III: DETAILED ASSESSMENT OF POLICY OPTIONS

The following tables set out policy options in a number of specific areas where operational objectives have been identified in section IV. In many cases, the operational objectives may address two or more of the problem drivers. However for the sake of avoiding repetition, the operational objectives are analysed under only one heading, on the understanding that certain options may also address other problem drivers.

I. Policy Options relating to Operational Objective 1 (Ensure that the EU approach is consistent with the approach followed at international level by extending the scope of application, strengthening and clarifying current requirements).

1. Tax Crimes: inclusion of tax crimes in the scope

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. General reference to tax crimes in the Directive, but without precise definition	+ Clear signal + Some degree of convergence + In line with Operational Objective 1 + Partially in line with Operational Objective 2	+ Some convergence will improve certainty	+ Coherent with policies aimed at reinforcing the fight against tax fraud and tax evasion
	- Risk of incoherent MS approaches	- Still some incoherence across MS risks burdens for cross-border business	
3. Make tax crimes a specific predicate offence and detail the circumstances in which the offence is committed	+ Clear signal + Coherence across MS + In line with Operational Objective 1 + Partially in line with Operational Objective 2	+ More efficient for cross-border business	+ Coherent with policies aimed at reinforcing the fight against tax fraud and tax evasion
	- lack of flexibility may create vulnerabilities	- Substantial difficulties to agree a common definition	- Risk to delay agreement on the full package

The revised international standards require that AML/CFT regimes incorporate "tax crimes" as a new predicate offence to money laundering. No further definition is given as to what "tax crimes" should mean. Three options are considered:

1. No change: this option would entail no additional cost and possibly be easy to agree politically. Given the existing "all serious crimes" approach in the current Directive[109], it could be argued that the existing approach in the Directive is already compliant with the new international standard. However such an approach might come at the cost of coherence between EU approaches on tax crimes, and the absence of explicit reference to tax crimes in the Directive might call into question whether the EU framework was really fully compliant with international standards.

2. Include a general reference to tax crimes in the Directive, but without a precise definition: this option would entail including a specific reference to tax crimes as a predicate offence. By using the existing threshold approach in the Directive (it is a serious crime if it is punishable by at least a maximum penalty of one year of deprivation of liberty), a degree of consistency across Member States would be achieved, although differences across jurisdictions would still remain – as is the case in most matters involving fiscal harmonisation. It would comply with the international standards and send a clear signal with respect to tax crimes.

3. Make tax crimes a specific predicate offence and detail the circumstances in which the offence is committed: this would be the optimal option with respect to meeting Internal Market goals. It would however go beyond the first operational objective of ensuring consistency with international standards, and would not be fully consistent with the second operational objective given the limited flexibility. It would potentially come at the cost of substantial delays due to political difficulties to agree on a common list of types of tax evasion behaviour which would need to be included. Such problems would risk jeopardising agreement on the broader AML/CFT legislative package, and compromise efforts to align the framework with international standards ahead of the FATF's Fourth Round evaluation process.

Stakeholders' views

The majority of stakeholders favoured explicit coverage of tax crimes, viewing this either as necessary, or not interfering with their national legislation (where the "all crimes approach" has already been introduced). Only around a quarter of respondents who expressed a view on this topic considered the existing provision to be sufficient. Almost all of these stakeholders would nevertheless support the inclusion of tax crimes as a predicate offence on condition that the definition was limited to "serious" tax crimes, possibly by applying a threshold, and that errors e.g. in completing tax compliance steps, as well as legitimate tax planning activities would not be included.

Conclusion

[109] Article 3.5 of the Third AMLD sets out a range of serious crimes that are considered to be criminal activities, and includes a general provision with respect to all other offences which carry a punishment imprisonment based on a maximum/minimum threshold

In view of the need to more clearly reflect tax crimes in the EU framework, but given the significant obstacles that would be faced with respect to securing agreement on a precise definition, the Commission has a clear preference for option 2, which although not achieving full consistency, will nevertheless achieve a degree of coherence between Member State approaches.

2. National Risk Assessments: Strengthen the requirement on Member States to identify assess, understand and mitigate ML/TF risks

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Introduce requirement for MS to carry out risk assessment, with option for supranational risk assessments in areas to be determined by EC (e.g. by AMLC, FIU platform, Europol).	+ Meets the objective + Each MS able to concentrate on their own risks	+ Flexibility allows MS some regional divergence + Can use national risk assessments to feed into EU-wide assessments as the concept matures	+ Use of supranational assessments brings convergence and contributes to the Internal Market
		- Costly supra-national elements	- Could be some fragmentation if each MS uses a different methodology
3. Introduce prescriptive set of measures to: • Carry out supranational risk assessment at EU level • Take specified action to mitigate risks at EU level	+ Meets objective	+Obliged entities have certainty	+ Greater convergence
	- Unless done comprehensively and regularly, could result in missing the objective	- Very costly supra-national risk assessment required - Needs to be kept up to date = resource intensive - Single approach not flexible	- Mandating action to be taken could lead to competitive disadvantage for the single market

The new FATF standards broaden the application of the RBA. At national level, countries are obliged to identify, assess and understand ML/TF risks, and to apply resources to mitigate those risks. Countries need to ensure that higher risks are identified and mitigated, but may permit simplified measures for certain requirements when lower risk has been identified. The FATF acknowledges that AML/CFT risk assessments at a supranational level should be taken into account. Three options on how to reflect the need for national/supranational risk assessments are considered:

1. No change: this option would entail no additional cost. However, as the existing EU rules contain very little about the need to understand and mitigate risks, it would leave the EU framework out of compliance with the international standards, and would likely result in different approaches being followed by Member States.

2. Introduce a new requirement in the Directive for Member States to carry out risk assessments at national level and take measures to mitigate risks, and introducing the possibility for supranational risk assessments to be undertaken in areas to be determined, based on detailed work to be undertaken at EU level (e.g. by AMLC, FIU Platform, Europol). Coordination could be provided at EU level, and

supranational approaches developed at EU level derived from the national risk assessments, in areas where risk factors common to the EU as a whole have been identified. This option, which recognises the fact that ML/TF risks facing jurisdictions are not always the same and need to be individually assessed, would meet the objective of strengthening the requirement to carry out national risk assessments. The approach would be fully in line with international standards, and would also recognise the specific supranational character of the European Union. However it would not achieve full convergence between Member States' risk assessments.

3. Introduce a prescriptive set of measures to carry out a supranational risk assessment at EU level and prescribe specified actions to mitigate risks at EU level: this option would treat the EU as a single jurisdiction, and would result in greater convergence between Member States' approaches. However it also carries a risk of missing the objective if the supranational risk assessment is incomplete or not updated regularly, and would be resource intensive and costly at EU level. Any inflexibility resulting from such an approach might expose the EU framework to criticism from international standard setters that risks were not being adequately and appropriately assessed.

Stakeholders' views

Stakeholders expressed strong support for the idea of broadening the application of the RBA. There was strong support amongst almost all respondents (public authorities, private sector and civil society stakeholders) who agreed with the general approach. Different views were however expressed as regards the usefulness of a complementary supranational assessment of the risk. Whereas a significant majority of public authorities were in favour, only a minority of respondents from the business segment supported such an idea. Most of the respondent companies and business federations expressed a preference for sufficient independence and flexibility to assess their own ML/FT risk, which would allow them to tailor adequate procedures taking into account the characteristics of the specific sector/product concerned.

Conclusion

In view of the need that risks will first and foremost need to be identified at national level, and in light of the complexities and inflexibility associated with a single EU supranational risk assessment, the Commission has a clear preference for option 2.

3a.Customer Due Diligence (risk based approach): Clarify when obliged entities must apply EDD and when they may apply SDD.

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. MS to ensure that EDD is conducted, with the option of allowing SDD to be conducted. Examples given of the risk factors to be taken into account.	+ Targeted approach to risk + Allows flexibility to respond to emerging threats	+ Targeted approach to dealing with risks will result in better mitigation + More cost-effective and efficient allocation of resources	+ Issuance of guidelines by ESAs will represent a cross-EU solution to an existing problem
	- Could be differences of interpretation	- Possible short-term costs of implementing systems	- Possible differential use of risk factors will give different risk profiles amongst obliged entities in different MS.
3. Prescriptive measures specifying when to carry out SDD and EDD and what measures to take.	+ Gives a consistent approach in the Directive	+ Some level of certainty	+ Arguably ensures a single approach
	- Solution does not target the risks involved, and thus the objective is not met in the longer-term	- Does not target risk - Would require a resource-intensive EU-wide risk assessment. - Resources of obliged entities could be spent on the wrong risks	- Need a full supra-national assessment of ML/TF risks in the EU

The current AML Directive recognises that enhanced and simplified CDD should be carried out in certain specified situations. However, the approach to simplified CDD has led to criticism in mutual evaluation reports of Member States, where the assessors interpreted the measures as requiring no CDD, as opposed to reduced CDD measures. The revisions to the FATF standards develop categories of risk factor that should be taken into account in determining whether enhanced CDD should be carried out, and whether simplified CDD may be carried out. Three options are considered:

1. No change to the existing Directive: this option would not properly address the deficiencies found in evaluation reports of Member States and would result in poor compliance ratings for MS going forward. In addition, the prescriptive measures are not commensurate to the risks posed, and thus are ineffective, with obliged entities having to channel resources to areas without commensurate risks.

2. An obligation on Member States to ensure that enhanced CDD is carried out in areas of high risk and an option for Member States to allow simplified CDD in lower risk situations, with examples of the factors to be considered (such as

geography, customer type, delivery channel etc.) would be a proportionate and flexible solution, allowing a targeted response to potential risks. In addition, this approach is in line with the greater emphasis on risk and the results of risk assessments that the revised FATF standards require. To address Internal Market concerns caused by the proliferation of different national approaches, work will need to be carried out by the ESAs in order to issue guidelines to Member States on risk factors.

3. A prescriptive listing of when to apply EDD and when SDD may be applied, accompanied by specific measures that must be taken would give some degree of certainty to the process, but would not be flexible enough to deal with the changing nature of ML/TF risks. In particular, the EU would need to carry out a thorough risk assessment across all Member States, and keep this up to date on an ongoing basis. This would be both costly and time-consuming, and would not give Member States an opportunity to respond to specific risks that they might be facing, even on a short-term basis.

Stakeholders' views

There was strong support for the idea that a more focussed and risk-targeted approach should apply with respect to EDD and SDD measures. The support was even stronger as regards the usefulness of establishing guidance on the application of such provisions. On the other hand, some companies and business federations were concerned that any clarification in the Directive should neither be exhaustive nor automatically lead to the assumption of ML/TF risks. In particular, these stakeholders pointed out the dangers of an overly rigid regime given the speed of innovation in some sectors (e.g. the payment sector) and the variety of products available.

Conclusion

In view of the need to tailor approaches to the specific risks on the basis of different risk factors, and to maintain an appropriate level of flexibility so as to be able to respond to emerging threats, and given that a targeted approach to risk allows more cost effective allocation of resources the Commission has a clear preference for option 2. The issuance of guidelines on risk factors by the ESAs will be an important element in promoting coherence of approach across Member States.

3b. Equivalent third countries: Clarify use of "equivalence" of third country regimes

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Remove the concept of positive "equivalence". Non-equivalence to be used as a factor/example of geographical risk..	+ Allows use of a risk-sensitive approach + Recognises that some third countries do not meet high EU standards	+ Some elements of risk assessment carried out across EU	+ Consistency of treatment of third countries across the EU
		- Resources will be needed to update the list of equivalent countries	- Possibility that it will be used differently across the EU
3. No equivalence process.	+ Consistent with risk-based approach	+ Avoids concentrating on one risk factor (i.e. geography)	
	- Does not give any certainty as to how the EU views third countries with "equivalent" regimes	- MS and some parts of the private sector report that equivalence process is useful	- Lack of convergence

The current AML Directive recognises the concept of third country "equivalence", whereby obliged entities are able to apply less onerous measures (for example, in relation to customer due diligence) to financial institution clients from "equivalent" third countries. This approach has been criticised in mutual evaluation reports as providing an automatic exemption from certain requirements, whilst not being founded on the basis of risk. Three options are considered:

1. No change to the existing Directive: this option would leave the uncertainty of the current provisions. This would not properly address the deficiencies found in evaluation reports of Member States and would result in poor compliance ratings for MS going forward.

2. This option would remove the concept of positive "equivalence" and introduce a concept whereby countries that are deemed to have AML systems that are not equivalent to those in the EU are treated as a factor or example to be taken into account by obliged entities when they are considering higher geographical risk alongside other risks, such as customer type and delivery channel. This would highlight the risk of doing business with customers in countries which do not have "equivalent" AML/CFT regimes to the EU, and would also make "non-equivalence" part of the overall risk package.

3. The complete removal of the "equivalence" process would leave Member States and obliged entities having to make their own decisions about risk. Although this would arguably be the most risk-sensitive approach, it would be the least convergent approach and would not recognise an exercise which some Member States and obliged entities find useful.

Stakeholders' views

Mixed views were expressed by stakeholders as to the usefulness of the listing process and its relevance in light of the revised FATF Recommendations' focus on a risk-based approach. The majority supported the listing process as useful (especially for smaller firms), whereas a minority felt that the current regime was of little benefit. Support for producing a binding list mainly came from the business sector while, according to several public authorities, such lists should rather be just one of a number of indicative factors of geographical risk.

Conclusion

Most stakeholders have expressed a desire to maintain an EU approach towards equivalence. However the current approach, which is based on Member State assessments which can result in automatic SDD for institutions from "equivalent" third countries, is not sufficiently risk-based. By focusing on pre-existing assessments made at international level on *non equivalent* regimes, and by ensuring that obliged entities treat this as a risk factor alongside other risks, a consistent approach can be ensured across the EU. The Commission therefore has a clear preference for option 2.

4. Supervision: Introduce more explicit recognition of RBA to supervision

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Recognise that supervision can be risk-sensitive, but leave the detail to be determined at sectoral level	+ Meets Operational Objectives 1 and 2 + Can target specific risks in each sector	+ Flexible detailed requirements can be changed more easily than revising a Directive + Can be informed by national and sectoral risk assessments	+ Consistent with International Standards
		- Some sectors do not have recognised colleges of supervisors (e.g. in the DNFBP sector)	- May still be elements of divergence between sectors/MS.
3. Supervisors given the power and complete discretion on how to supervise all sectors	+ Fully risk-sensitive + Fully in line with Operational Objective 1 (better fits to the FATF standards)	+ Allows greater degree of targeting, therefore improved efficiency	+ Consistent with International Standards
	- Not in line with Operational Objective 2 (Lack of convergence)	- Different approach will create inconsistencies and increase costs across borders	- Impact on Internal Market

The Third AML Directive requires obliged entities to be "effectively monitored". The revised FATF standards give specific recognition that supervision of institutions and persons covered by the Recommendations can be carried out on a risk-sensitive basis. This allows resources to be targeted at areas where risks are thought to be higher.

Three options are considered:

1. No change to the existing provision: supervisors would be able to continue with existing approaches, although those that already use elements of risk-sensitivity would not necessarily be able to make use of the provisions in the revised FATF standards. Depending on the Member State's interpretation of "effectively monitor", resources might not be used efficiently.

2. Limit the approach in the Directive to a specific recognition that supervision should be carried out on a risk-sensitive basis, with a link made to national and sectoral risk assessments to ensure that the risks are adequately captured, and give a role to the ESAs to develop more detailed measures. This option would allow supervisors to adopt approaches which are more targeted towards risk. The concept would, however, be more appropriate in developed sectors (such as banking, securities and insurance

supervision), and less so in certain DNFBP sectors where a sectoral approach at EU level might not be viable.

3. Allow full discretion for supervisors to apply a risk-sensitive approach to supervision, without any additional measures at EU level as described under option 2. This option would maximise flexibility for all supervisors, but would potentially lead to a lack of convergence as each sector in each Member State would be supervised according to different risks and principles.

Stakeholders' views

Among the few respondents who expressed a clear view on this topic, there was broad consensus in recognition of the importance of risk-based supervision. With respect to supervision of cross-border activities, the business sector was concerned that the minimum harmonisation approach should avoid that scope and application substantially differ across Member States, and strongly supported the provision of sectoral guidance. Some stakeholders also suggested that supervision should focus on less-developed sectors, rather than on high-risk entities which, very often, were better equipped and had more experience in facing the specific ML/FT risks.

Conclusion

In view of the need to reflect the new international standards, maintain a degree of consistency between EU supervisory approaches whilst permitting an appropriate level of flexibility in implementation, the Commission has a clear preference for option 2.

5. Politically Exposed Persons (PEPs): Broaden existing approach to treatment of politically exposed persons (PEPs) to cover domestic PEPs and PEPs working in international organisations on a risk-sensitive basis

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Introduce requirements for domestic PEPs/PEPs in international organisations with risk-sensitive elements	+ Meets objective of widening scope + Complies Operational Objective 1	+ Addresses highest risk (foreign PEPs) and allow a graduated approach to other PEPs	+ Consistent with international standards
		- Differential approach may lead to inconsistencies	
3. Extend provisions for international PEPs to domestic PEPs and PEPs in international organisations	+Meets objective + Requirement goes some way to Operational Objective 3.	+ Clarity in requirement	
	- Goes further than objective	- Costly for industry, without corresponding benefit	- Goes further than international standard

The existing EU standards were aimed at PEPs residing in a third country, and require a certain level of enhanced due diligence to be performed. The revised FATF standards have expanded the definition to include domestic PEPs and PEPs working in international organisations, with enhanced measures to be taken on a risk-sensitive basis.

Three options are considered:

1. No change: although this option would mean the least cost to industry, it would result in EU legislation being below the international standards, and Member States would risk poor compliance ratings in mutual evaluation reports. In addition it would not address an area of potential risk.

2. Introducing provisions for domestic PEPs/PEPs working in international organisations, with risk-sensitive measures to be taken: this option is more in-line with the international standards, and addresses the risks posed by PEPs domestically and those working in international organisations, who might have access to proceeds obtained corruptly. However, as not all PEPs are automatically higher risk, a risk-sensitive element would be introduced to allow obliged entities to assess the risks that they pose and to apply appropriate mitigating measures, without interfering with the current need to apply higher requirements for foreign PEPs. The differential approach might cause some confusion for obliged entities, who would need to apply different standards to different categories of PEP.

3. Extend the existing provisions (i.e. a requirement for EDD measures) to all types of PEPs: requiring a certain level of enhanced due diligence to be conducted for each category of PEP would give a degree of consistency to the provisions, and would place the EU ahead of the international standard. However, the cost of this requirement to industry would arguably outweigh the potential benefit, with obliged entities being required to apply enhanced due diligence to all categories of PEP regardless of the risk. This would involve a potential waste of resources.

Stakeholders' views

The idea of extending the Directive to domestic PEPs and PEPs working in international organisations was fully supported by public authorities, representatives of liberal professions and civil society. Support also came from the business sector (financial and non-financial), which however remained concerned about the significant difficulties faced when identifying PEPs. These respondents therefore expressed a wish to see a clearer and narrower definition, a broader application of the RBA and the provision of a centralised, up-to-date and reliable PEPs lists.

Conclusion

In view of the heavy cost implications that the approach under option 3 would entail, and given that the approach in option 2 would still be consistent with international standards by addressing the highest risk (foreign) PEPs while allowing a graduated approach for other types of PEPs, the Commission has a clear preference for option 2.

6. Availability of beneficial ownership information: Enhance the public availability of information on the beneficial owner / enhance the transparency of legal persons and legal arrangements

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Requirement on companies to hold information on BO and to make this information available to competent authorities and obliged entities	+ Enhanced transparency + In line with Operational Objective 1	+ Limited additional cost and easy to set up for companies, + Relieves the current burden on obliged entities	+ In line with Commission's EU Internal Security Strategy + In line with international standards
	- Less public transparency than option 3	- Cost on companies, especially for those with a complex structure	
3. Require public availability of information on shareholders, BO and nominees through a public register	+ Enhanced transparency + Meets demand for transparency from civil society and European Parliament	+ Relieves the current burden on obliged entities	+ In line with international standards
	- Challenge to maintain up-to-date information	- Shifts burden (costs) onto Member States	- may raise data protection concerns

The new FATF standards require countries to ensure that there is a set of basic information on the company available in business registries and/or held by the company itself and made available to competent authorities. Access by covered institutions to this information should be facilitated. Further transparency of nominee shares or directors is also required (disclosure of identity or licensing). Countries can choose between several mechanisms. For legal arrangements, the standards recognise the role of the trustee as holder of the beneficial owner information and introduce a requirement for trustees to disclose their status when they engage with reporting parties. The current Directive does not provide explicit provisions. Calls for more transparency also come from the 2010 Commission's Internal Security Strategy[110]and the European Parliament[111].

Three options are considered:

1. No change: this option would not be effective as it would not allow for greater transparency on beneficial owner and legal persons and arrangements. It would not be in line with new FATF standards.

110 Commission Communication: "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM (2010)673 final.

111 European Parliament Resolution of 15 September 2011 on the EU's efforts to combat corruption. It called for rules to "make the fight against anonymous shell companies in secrecy jurisdictions (…) a key element of the upcoming reform of the Anti-Money Laundering Directive

2. Require Member States to require companies[112] to hold and up-date information on their beneficial owners and to make this information available to competent authorities and entities covered by the Directive. This option would allow greater transparency of information on the ultimate beneficial owner of companies. They are best placed to understand their own beneficial ownership, and making the information available to obliged entities would be a useful tool in the CDD process. Some cost would be involved in recording and maintaining this information, and making it available upon request. Finally, this option would be in line with international standards and Commission's EU Internal security strategy.

3. Require Member States to set up public registries on shareholders as well as on beneficial owners, in addition to the same information held by companies. This option would be the most effective as regards the level of transparency and would meet the demands from civil society and European Parliament to promote greater public access to beneficial ownership information. As with option 2, it would relieve the burden on obliged entities and would be in line with international standards and the Commission's strategy. But an agreement of Member States could be difficult to obtain given the new burdens it would place on them, and general availability of such information may raise data protection concerns. At least public availability of shareholder information should be provided, which is already a reality in most Member States.

Stakeholders' views

There was strong support among stakeholders to include in the Directive measures to promote the transparency of legal ownership. Views differed, however, as to the means to achieve it. A majority of those who expressed an opinion stressed the need for an official, timely up-to-date and reliable source of information, possibly through national registries. Others suggested that a centralised database should be created at EU level and access made available to obliged entities. Some respondents argued that beneficial owners should be declared when registering a legal entity, and given advanced warning about the possible data protection implications.

Conclusion

In view of the fact that option 2 already goes beyond the international standards, it should be relatively straightforward to achieve, keep compliance costs for companies relatively low but at the same time represent a significant benefit for obliged entities, the Commission has a clear preference for option 2.

[112] In the case of express trusts, in accordance with the international standards, there should be a requirement to identify the settlor, trustee, protector, the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust, and to hold that information.

7. Electronic fund transfers: Enhance detection of misuse by terrorists and criminals of electronic fund transfers

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. Maintain current approach	0	0	0
	0	0	0
2. Make changes to the FTR to introduce requirement to include information on the beneficiary and limit exemptions from scope	+ Improves detection by enhancing traceability of electronic fund transfers + In line with Operational Objectives 1 and 2		+ In line with EU Strategy on Terrorist Financing
	- Electronic fund transfers below €1,000 are not subject to identity verification	- Limited additional costs for business due to adaptation of payment systems	
3. Require beneficiary and payer information to accompany the payment and require identity verification as of €0	+ Improves detection by enhancing traceability of electronic fund transfers		+ Exceeds international standards
	- May drive certain transactions to unregulated PSPs - Not in line with Operational Objective 2 (flexibility)	- Additional costs for non-account based payment service providers	

The new FATF standards seek to enhance the transparency and traceability of electronic fund transfers by requiring the inclusion of information about the beneficiary in wire transfers, as well as an explicit obligation to take freezing action with respect to UN Resolutions and to prohibit conducting transactions with designated persons and entities. There are specific obligations on money or value transfer service providers (MVTS), in particular a requirement to file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Three options are considered:

1. No change: this option would not be effective as it would be inconsistent with the new FATF standards, and it would leave gaps with respect to traceability of electronic fund transfers. Since this is an area governed by an EU regulation, no facility to correct this deficiency at national level would be possible, and EU Member States' legislation would be rated non-compliant with the international standard, with corresponding reputational damage to the EU's financial system and its institutions.

2. Make changes to the Fund Transfers Regulation (FTR) to introduce a requirement to include information on the beneficiary and other key changes resulting from the revised international standard: this option would not entail significant adjustment costs, as most fund transfers already contain information on the beneficiary and so would not be affected. Ensuring that beneficiary information is included in all electronic fund transfers would provide an effective tool for law enforcement and ensure full traceability of all transfers, although transfers below €1,000 do not require identity verification.

3. Require beneficiary and payer information to accompany the payment and require identity verification as of €0 as opposed to the existing threshold of €1,000: this option would be the most effective way of ensuring full traceability of electronic fund transfers. However customer verification would entail significant additional costs for lower value transfers, increasing the costs for the end users and potentially driving parts of the payments business to more risky unregulated payment channels. This option would exceed the international requirements.

Stakeholders' views

The few comments received on this topic showed a divergence of views according to the different categories of respondents. Whereas some public authorities considered it appropriate to reduce the current thresholds in respect of electronic fund transfers (from the current € 1,000 threshold), business sector respondents (mainly financial services) considered the current amount appropriate and argued that lowering this threshold would have limited effects and disproportionate costs for the financial institutions.

Conclusion

In view of the fact that option 2 achieves the objectives of consistency with international standards without significant burdens for obliged entities, and that option 3 would introduce a substantial new compliance burden (albeit representing an enhancement to the possibility to trace transactions), the Commission has a clear preference for option 2.

II. Policy Options relating to Operational Objective 2 (Ensure consistency between national rules and where appropriate flexibility in their implementation by strengthening and clarifying current requirements).

7. Improve comparability of statistical data

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. Maintain current approach	0	0	0
	0	0	0
2. Provide further guidance on how reporting by MS should be carried out	+ Might help improve the ability to measure effectiveness of the EU framework + In line with Operational Objective 1 and 2		
	- Comparability across MS will remain difficult	- Limited additional costs for MS	
3. Reinforce the requirement under Art. 33 of the 3AMLD with respect to statistical data	+ Improves the ability to measure effectiveness of the EU framework by imposing on MS more explicit requirements on comparability and sharing of information + In line with Operational Objective 1 and 2		+ Coherent with the Hague programme mandate
	- Comparability across MS will remain difficult unless underlying approaches (e.g. the notion of an STR) are also harmonised	- Limited additional costs for MS	

Article 33 of the Third AMLD imposes an obligation on Member States to maintain and publish comprehensive statistics, so that they are in a position to review the effectiveness of their AML/CFT systems. However significant definitional and systemic differences (e.g. different notions of what constitutes a "report", different processing of reports, and different approaches towards prosecution of cases) considerably undermine comparability across countries and complicate assessment of the extent to which AML/CFT systems are effective.

Three options are considered:

1. No change: this option would entail no additional cost. However it would not achieve the objective of comparability across the EU and would mean that an overall

assessment of the EU framework would remain very difficult. Moreover, given that certain parts of the EU framework may be subject to supranational assessment by the FATF in the future, there is a risk that the EU statistical framework to measure effectiveness would fall short of the international standards. The current degree of flexibility that the AMLD allows has affected the comparability of statistical data, due to legal, operational and statistical reasons.

2. Provide further guidance on how reporting by Member States should be carried out with a view to achieving more coherence between data sets. This option would not entail changes to the Directive, as Article 33 already contains minimum requirements on statistical reporting. Further Guidance issued by the Commission, building on the first statistical exercise (see "*Money Laundering in Europe"*[113]) could serve to improve the consistency of reporting of effectiveness indicators across the EU, and facilitate an evaluation of the effectiveness of the EU AML/CFT framework as a whole. However the underlying differences with respect to AML approaches (e.g. the form of the reports differs significantly, the different definitions as to what constitutes a predicate offence, different procedures on handling information, etc.) would remain and continue to complicate cross-border comparability. However as the existing minimum requirements (especially in Article 33.1) imposed on Member States are not sufficiently detailed, this has led to difficulties to obtain comparable data across Member States. Such problems may not be addressed solely through the issuance of additional guidance.
3. Reinforce the requirement under Article 33 with respect to statistical data in order to ensure more comprehensive and comparable statistics in compliance with the Action Plan "Measuring Crime in the EU: Statistics Action Plan 2011- 2015". This option would consist in operationalizing Article 33 (1), by notably linking it with the necessary national risk assessment. Article 33(2) could be amended in order to make more explicit the data requirements . Further guidance of important effectiveness indicators across the EU in similar ways to those described under option 2 could be provided. This approach might enhance comparability of important effectiveness indicators across the EU in similar ways to those described under option 2. However, as also described under option 2, comparability across Member States would still remain impaired as a result of underlying differences with respect to AML approaches.

Stakeholders' views

Many respondents to the Commission's consultation supported greater harmonisation of the reporting regime across the EU, in order to improve effectiveness.

Conclusion

113 ISSN 1977-0375, Eurostat Methodologies and Working Papers, Cynthia Tavares, Geoffrey Thomas and Mickaël Roudaut, 2010 edition.

In view of the fact that Member States have inconsistently implemented the requirements in Article 33, further clarification of the requirements appears necessary in the Directive. For this reason, the Commission has a clear preference for option 3.

8. Identification of the "beneficial owner", including clarification of 25% ownership threshold

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Retain 25% threshold but clarify requirements for holding companies. Leave open for guidance by ESAs.	+ Meets objective of clarification + ESAs best placed to provide further clarification	+ Threshold gives a framework for obliged entities + In line with company law concept of ownership + Flexibility for guidance by ESAs	+ Coherent with Internal Market
	- Converged national approaches in line with Operational Objective 2	- Concentration on threshold may not always find the ultimate beneficial owner.	
3. Remove threshold and replace with requirement to always find natural person who owns/controls company	+ Targets the potential risk (i.e. person who controls company) + Exceeds Operational Objective 1 + Requirement goes some way to meeting Operational Objective 3.	+ More focussed towards the actual risk	
	- Could lack clarity unless detailed guidance is prepared - possible conflict with Operational Objective 2.	- Costly for industry	- Greater risk of diverging implementation across MS

Existing EU legislation defines beneficial owner as "the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted". When beneficial ownership can be ascertained through share ownership, a 25% plus 1 share threshold is given as evidence of direct or indirect ownership. However, a report by the AMLC has identified issues in relation to how the 25% threshold is interpreted in Member States.

Three options are considered:

1. No change would mean that obliged entities would not need to adjust their systems. However, the inconsistency of interpretation across Member States has already led to a lack of convergence, and thus this is not the preferred option.

2. Maintain the approach which requires identification of the BO as of a 25% ownership threshold, but clarify what the "25% threshold" refers to, particularly in relation to holding companies and foundations. This option would address the issue of inconsistency and lead to greater convergence. The precise nature of the requirement could be left for clarification in guidance by the ESAs where related issues such as the clarification of the relationship between "ownership" and "control", "multi-layer corporate vehicle structures", and "close associate" could also be tackled. There should, however, be a clear understanding that the 25% threshold is a minimum standard, and not a replacement for the requirement to find the ultimate beneficial owner where doubts exist that shareholding alone is sufficient. For example, reporting entities could be required, when confronted with suspicious circumstances, to undertake further inquiry to identify and record information on other parties who appear relevant (the "close associate" i.e. the typical frontman) to find out whether other natural persons beyond the formal legally declared owners really are in control.

3. Remove the existing 25% threshold and replace it with a stricter requirement to always find the natural person who owns/controls the company. This option would require obliged entities to focus more on the actual risk posed by persons who control companies. However, it would lead to greater expense for obliged entities and a lack of guidance as to what was expected could lead to a lack of convergence across Member States, who might interpret the person who "controls" a company differently.

Stakeholders' views

A substantial majority of stakeholders commenting on this issue shared the view that the 25% threshold appears appropriate and should be maintained. The support was even stronger as regards the usefulness of improving legal certainty across the EU about who the beneficial owner is, while maintaining a risk-based approach to identifying, and verifying the identity of beneficial owners.

Conclusion

In view of the fact that option 2 would be the best way to ensure greater convergence between Member State approaches, and given that the ESAs are best placed to carry forward work in this area, the Commission has a clear preference for option 2.

9. Clarify responsibilities for AML supervision between the home and host supervisors

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Clarify in the Directive	+ Establishes a clear legal footing for supervisors + Increased clarity for business + More efficient detection of ML/TF by FIUs + Fulfils Operational Objectives 2 and 3	+ Clarity and coherence across Member States facilitates the business environment	+ Coherent with International Standards
	- Reduced flexibility for MS	- Introducing a requirement to report suspicions where they arise risks adding burdens for cross-border market operators	- Potential Conflicts with Internal Market would need to be addressed

Article 37 of the Third AMLD obliges Member States to require competent authorities to monitor and take measures to ensure compliance with the requirements of the Directive by obliged persons and institutions.

Public stakeholders, especially supervisory authorities, have expressed concerns about the lack of legal certainty in the current legislative texts about their ability to ensure correct compliance with host state AML/CFT obligations in the case of payment service and E-Money providers, operating on the basis of a single EU passport via branches or agencies. Such uncertainties have the potential to create gaps in compliance and might undermine the effectiveness of the framework.

Two options are considered:

1. No change: the Commission has already published a staff working document which clarifies the articulation between the Payment Services Directive and the Third AMLD. However stakeholders – especially public authorities – have complained that the staff working document does not provide sufficient legal certainty, as it is not legally binding. It would therefore fall short of providing both supervisors and obliged entities with legal certainty, and may not resolve persisting uncertainties which complicate cross-border business on the basis of a single passport

2. Clarify in the Directive: this option would build on the existing clarifications contained in the Commission's staff working document, and establish rules on a firm

legal footing, thus providing certainty for supervisors and obliged entities about how AML compliance may be achieved so that host state rules are respected, while ensuring no undue hindrance to the cross border provision of services by licenced entities. The introduction of a requirement to file STRs to the FIU in whose territory the institution or person forwarding the information is situated will lead to improved detectability of ML/TF by FIUs, and should not impose additional burdens for cross-border businesses.

Stakeholders' views

All stakeholders responding on this issue were in favour of clarifying the regulatory powers which home and host AML/CFT supervisors have in cross-border situations. In particular, many respondents highlighted the need to consider such powers with regard to payment and e-money institutions, their agents and, where applicable, their distributors. Support for recognising the host country's power to directly supervise and, where need be, prosecute breaches of AML/CFT provisions occurring on its territory (including cases of non-compliance with CDD procedures and insufficient ST/SA reporting) came from several public authorities. The business segment, although in favour of clarifying supervisor authorities' powers in cross-border situations, was of the view that duplicating regulatory obligations by requiring compliance to local AML provisions creates additional costs. These respondents therefore envisaged greater co-operation, information sharing and possible delegation of powers between home and host AML/CFT supervisors.

Conclusion

In view of the fact that there is a need to respond to stakeholders' concerns for greater legal certainty in ways which would both clarify responsibilities of AML supervisors as well as the requirements on cross-border businesses, the Commission has a clear preference for option 2.

10. Strengthen and converge administrative measures and sanctions for obliged entities not complying with the requirements of the Directive

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Introduce a set of common principles-based rules to strengthen administrative sanctions	+ Improved compliance by obliged entities + Enhanced comparability between MS + In line with the General Objectives	+ A more level playing field + Coherence across Member States facilitates the business environment	+ In line with Commission's policy on strengthened financial services sanctions
	- Less flexibility for MS	- Adjustment costs	
3. Introduce common rules on sanctions, setting the minimum level of sanction according to different offences and for each category of administrative fine.		+ A fully level playing field + Coherence across Member States facilitates the business environment	+ In line with Commission's policy on strengthened financial services sanctions
	- No flexibility for MS - Not fully in line with Operational Objective 2	- Challenging to agree as legal systems and traditions vary considerably	

The Commission's Communication "Reinforcing sanctioning regimes in the financial sector" of 8 December 2010 sets out core principles that should apply to sanctions on financial institutions. The objective is to reinforce the efficiency and convergence of the sanctioning regimes, in order to strengthen the Single Market. Strengthening sanctioning regimes was also one of the elements of the financial sector reform at international level. According to the Commission's policy, standard provisions are to be incorporated into all Directives related to Financial Services. Elements include: the requirement to have a set of core administrative sanctions for key infringements; publication of sanctions as a rule; a sufficiently high level of administrative fines (not less than obtained benefits); harmonisation of criteria to determine the sanction; ensuring that authorities have the necessary powers when dealing with cross-border cases. Certain of these standard clauses might not be adequate for AML/CFT purposes, and the policy will need to be tailored to the specific needs of the sector.

Three options on how to strengthen and converge national rules are considered:

1. No change: this option would entail no additional cost. However it would not contribute to a reinforcing of AML/CFT compliance by obliged entities and would not be in line with the Commission's Communication "Reinforcing sanctioning regimes in

the financial services sector". The playing field among obliged entities from different Member States would remain unlevel.

2. Introduce a set of common principles-based rules to strengthen administrative sanctions, along the lines of the Commission's policy as outlined in its Communication 'Reinforcing sanctioning regimes in the financial services sector: this option would enhance effectiveness of the AML/CFT regime by improving compliance by obliged entities and allowing for a more consistent approach across Member thereby ensuring a greater level playing field for EU companies and facilitating the business environment. Some adjustment costs would be incurred, and a degree of flexibility for Member States would be curtailed.

3. Introduce a detailed set of prescriptive rules, (e.g. setting the minimum level of sanctions according to different offences and for each category of administrative fine): this option would fulfil the same objectives as option 2. However, it would reduce flexibility for Member States (not fully in line with Operational Objective 2). As legal systems and traditions vary considerably within the EU, it could be prove difficult in practice to agree on a fully harmonized sanctioning regime.

Stakeholders' views

Around one quarter of respondents expressed a view on this issue. A majority were in favour of greater harmonisation of the sanctioning regime across Member States. Support came in particular from the business sector, on the grounds that there was a need to ensure a common/uniform application of the administrative sanctions regime, in order to avoid that one national system might be more favourable than another. It was also argued that providing more powers and sanctions for AML/CFT purposes would send the right message that was currently lacking. Public authorities were also supportive, stressing that harmonisation would be an efficient tool for the prevention of regulatory arbitrage. However, it was also argued that while it would be useful for all Member States to have a legal basis to apply countermeasures when they considered it appropriate to do so, rigid prescription of such countermeasures at EU level would greatly undermine the risk-based approach and would be against the principle of subsidiarity.

Conclusion

In view of the need to strengthen sanctions with a view to more effective enforcement of the rules, but given that systems in place in the Member States function very differently, a flexible not overly-prescriptive approach appears the most appropriate. For these reasons the Commission has a clear preference for option 2.

III. Policy Options relating to Operational Objective 3 (Ensure that the rules are risk-focussed and adjusted to address new emerging threats, by strengthening and clarifying current requirements).

11. Broaden the scope to cover the gambling sector and address new threats

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. Maintain current approach	0	0	0
	0	0	0
2. Change scope to cover the gambling sector based on a broad definition – exemptions only if there is a very low risk of ML/TF	+ Enhances effectiveness of the fight against ML/TF + Levels the playing field with non-obliged gambling sector + Exceeds Operational Objective 1 + In line with Operational Objectives 2 and 3	+ Simpler to apply + Risk based approach allows exemptions in cases of very low ML/TF risks	+ Consistent with the Internal Market
		- Additional costs to sectors not currently covered by the framework -Additional costs to supervise	
3. Change the scope to cover gambling activities where there is a proven higher risk	+ Enhances effectiveness of the fight against ML/TF + Levels the playing field with non-obliged gambling sector + Exceeds Operational Objective 1	+ No costs for gambling activities which are not identified as higher risk	
	- Less flexible to emergence of new risks - Not fully in line with Operational Objectives 2 and 3	- More complex to apply due to need for identification of higher risk activities - Additional costs to sectors not currently covered by the framework - Additional costs to supervise	- Requires a supranational assessment of risk

The Third AMLD includes "casinos" within its scope but without providing any definition. Activities "performed" on the Internet (recital 14) are also covered. There are concerns that the absence of a clear definition leads to different approaches at national level, and leaves important areas of the gambling business which may be particularly vulnerable to AML/CFT outside the scope of the preventative framework.

Three options are considered:

1. No change: this option would entail no additional costs for the as yet uncovered gambling sector, however the ML/TF vulnerabilities would remain, as would the costs of cross-border compliance resulting from different national regulatory approaches. The playing field for AML regulated vs. non AML regulated gambling activities would remain unlevel.

2. Broaden the scope of the Directive beyond "casinos" to cover the gambling sector, based on a broad definition of gambling. The scope for exemptions from coverage would be limited only to circumstances where there is a very low risk of ML/TF: this option would entail costs for those higher risk gambling businesses not currently caught by the existing AML/CFT framework (e.g. sports betting, betting shops, lotteries, etc.). Introducing AML/CFT systems entails high compliance costs – especially in terms of the initial investment needed. It is much harder, on the other hand, to estimate the potential benefits of closing down an important avenue of money laundering to organised crime.

3. Broaden the scope of the Directive beyond "casinos", but include only those gambling activities where there is a proven higher risk: this option would be impose no costs on certain gambling businesses which remained outside the scope of the Directive. However identifying which types of activity are not higher risk may in practice be difficult, and the approach may not be flexible enough to respond to market changes which result in the emergence of new, unforeseen risks.

Stakeholders' views

Almost one third of respondents expressed views on this topic. There was strong support to include gambling, and to ensure that it covered both land-based and on-line gambling activities (including e.g. sports betting, horse racing and lottery games). Most of those respondents stressed the need for a risk-based approach (which in their view would therefore exclude e.g. arcades, kiosks and gas stations from the scope of the Directive). Most respondents from the gambling sector also pointed that such an extension would imply provisions on CDD and supervision would need to be adapted in light of the specificities of on-line and land-based gaming activities other than traditional casinos.

Conclusion

In view of the need to address threats of money laundering in the gambling sector more broadly than the current limitation to casinos, and in view of the fact that applying a broad

definition of the scope of gambling would be more straightforward than attempting to determine at EU level which specific areas of gambling might be considered higher risk (such an assessment might vary across jurisdictions) the Commission has a clear preference for option 2.

12. Clarify application of data protection rules in the context of AML/CFT

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Require MS to clarify interaction between AML/CFT and DP rules at national level	+ Reduced uncertainties for entities; better compliance with AML and data protection requirements + Enhanced level of respect of data protection rules + In line with Operational Objectives 1 and 3	+ Member State authorities would retain flexibility	
	- Incoherence across Member States		- Not in line with Internal Market
3. Introduce new rules in the AML Directive to clarify interaction, in particular as regards data retention and data sharing within the groups	+ Enhanced coherence across Member States; + Reduced uncertainties for entities; better compliance with AML and data protection requirements + AML group-wide compliance facilitated + In line with all Operational Objectives	+ Cost savings for groups	+ In line with Internal Market + In line with International Standards + In line with Commission's Data protection proposals
	- Data sharing with third countries whose DP regimes have not been recognised likely to remain problematic	- Possibly difficult to agree on a wording which reflects an appropriate balance between AML and DP objectives	

Private stakeholders point to a number of practical difficulties as regards their ability to comply with AML requirements while at the same time adhering to rules aimed at ensuring a high level of protection of personal data. These difficulties include sharing of information within the group or between FIUs, screening on the basis of non-EU sanctions lists, consent of the data subject, record keeping, and legal uncertainties with regard to processing of AML/CFT related data within entities. The recently proposed EU Regulation and Directive on data protection[114] are aimed at strengthening and clarifying data protection rules and might

114 Commission's data protection proposals (COM(2012) 11 final) and (COM(2012) 10 final). http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

need to be clarified in the revised AML/CFT legal framework. In its Opinion 14/2011[115], the Article 29 data protection working party called for more detailed consideration of data protection issues in the AML legislation, in particular as regards retention of personal data. One particular issue is the requirement, reinforced by the new FATF standard, to implement at a group level AML/CFT programmes, including policies and procedures for sharing information within the group. Within the EU, institutions experience in practice some restrictions from local data protection authorities to the sharing of data (e.g. restrictions to information sharing on STRs, to information flows to the auditors of the Head Office). Data sharing with third countries whose data protection regimes are not considered adequate may raise other difficulties.

1. No change: this option would entail no additional costs. However obliged entities would continue to experience difficulties in their AML compliance all the more so as reinforced rights stemming from the new EU data protection proposals (e.g. a reinforced right to be forgotten, information about data security breaches) could lead to new legal uncertainties. Inconsistency across Member States would continue to exist, leading to uneven level playing field. As regards data sharing within the groups, institutions will continue to experience legal uncertainties and practical difficulties.

2. Require Member States to clarify interaction between AML/CFT and data protection rules at national level (e.g. by issuing guidance, setting up a dialogue between data protection and AML/CFT authorities, or introducing specific rules into national AML laws): this option would help reduce legal uncertainties to which businesses are confronted in their day-to-day operations and therefore enhance their compliance with AML rules while at the same time ensuring compliance with a high level of data protection. However, incoherence across Member States would continue to exist as a result of differing national interpretations, implying costs for cross-border businesses and complications for groups operating cross-border group compliance of AML/CFT programmes. As regards the particular issue of data sharing within the group, this option would not bring a satisfactory solution. Indeed, if clarification is offered only at national level, entities of the groups established in different Member States might still not be able to share data due to inconsistencies in national legislations/practices of national data protection authorities.

3. Introduce new rules in the AML Directive to clarify the interaction between AML/CFT and data protection rules: this option would help reduce legal uncertainties to which businesses are confronted in their day-to-day operations and notably facilitate cross-border group compliance of AML/CFT programmes, which would be in line with the new international standards. New provisions might clarify how long data can be held by obliged entities, the circumstances under which data can be transferred to third countries, and ensure that data collected for AML/CFT purposes cannot be processed for commercial purposes.

---

115 Opinion 14/2011on data protection issues related to the prevention of money laundering and terrorist financing, 01008/2011/EN, WP 186, 13 June 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp186_en.pdf

Stakeholders' views

Many stakeholders complained that national data protection rules impacted effective intra-group transfer of information – this was one of the most important factors generating administrative burdens and reducing the effectiveness of AML procedures. The business sector also warned about three further issues:

- under the current data protection regime, there are serious restrictions on disclosure and transfer of personal data to third country public authorities;
- there are difficulties with respect to data retention periods;
- under the proposal for a data protection Regulation, it is not clear how the empowerment to introduce restrictions of data protection principles will be interpreted.

There was unanimous recognition of the need to address these issues by ensuring effectiveness in monitoring and reporting in ways which would not breach data protection principles. Diverging opinions were however expressed on the right way forward. Support for the idea of introducing more detailed data protection provisions for AML/CFT purposes was particularly strong from business.

Conclusion

In view of the need to ensure a high level of data protection whilst at the same time ensuring proper compliance with AML rules, it appears appropriate to ensure an adequate legal basis for data processing in specific AML legislation. This would be best achieved within an EU Directive, as opposed to in national legislation, as this would be the best way of ensuring coherence across Member States and facilitating personal data sharing for AML purposes across groups (particularly across borders). For these reasons, the Commission has a clear preference for option 3.

13. Threshold for traders in high value goods: Strengthen the preventive measures

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0
2. Reduce the threshold (scope and requirement to conduct CDD to €7,500)	+ Addresses risk of use of cash + Exceeds Operational Objective 1 + In line with Operational Objectives 2 and 3	+ Targets the black economy	+ Brings threshold more in line with common practice in MS + Compliments policies aimed at the free movement of persons + Shows EU response to address actual ML concerns
		- May bring more obliged entities into scope, or push them towards accepting other payment means, with potential cost implications	
3. Reduce the threshold (scope and requirement to conduct CDD) to zero	+ Firm controls on the use of cash + Exceeds Operational Objective 1 + In line with Operational Objectives 2 and 3	+ Targets the black economy	+ Single threshold would promote certainty + Compliments policies aimed at the free movement of persons
	- Risks driving the use of cash underground - Financial inclusion impacts	- May bring more obliged entities into scope, or push them to accepting other payment means, with potential cost implications - Challenging to monitor compliance	- Singles out this sector for more stringent rules

The existing Directive covers natural or legal persons trading in goods but only if they accept cash payments of €15,000 or more. CDD is required for occasional transactions above this amount. Evidence suggests that some Member States are applying lower thresholds, which has resulted in driving the use of traders for the purposes of laundering the proceeds of robberies to other Member States.

Three options are considered:

1. No change: this option would mean no change in the numbers of traders brought into scope and no change to the threshold for CDD. Although this would be the least costly option, it would fail to address risks identified by a Member State.

2. Reducing the scope and CDD thresholds to €7,500[116]: this option would bring more traders into the scope of the Directive, and mean that they would need to apply CDD measures for cash transactions of €7,500 and above. This lower threshold would potentially bring a larger number of traders into the scope of the Directive, and may mean that CDD would be carried out for more transactions, or alternatively that the number of cash transactions actually executed above €7,500 would be considerably reduced as traders insisted on other means of payment. This option would address concerns about the use of cash in the black economy as well as that the higher threshold has resulted in the proceeds of robberies from one Member State (which has lowered the threshold) being laundered in other Member States with higher thresholds. This would reduce the attractiveness of using the sector in the EU to launder criminal proceeds.

3. Reducing the scope and CDD thresholds to zero for specified obliged entities (e.g. dealers in precious metals and stones, second hand car dealers, auction houses): while it would be effective in limiting the use of cash, the inconvenience and potential costs may be disproportionate as compared with the perceived benefit. Effectively requiring AML controls for all transactions (especially CDD) could drive the use of cash into the unregulated sector and could have impacts on financial inclusion. It would also prove challenging and resource intensive for competent authorities to ensure compliance.

Stakeholders' views

The opinions expressed on this issue diverged according to the different categories of respondents. Whereas several public authorities considered it appropriate to reduce the current thresholds in respect of occasional transactions (suggestion was made, for example, to substitute the current € 15,000 threshold to a minimum € 1.000 threshold, or even to a € 1 threshold in case of payment in cash, or via a prepaid card), the majority of respondents from the business segment (mainly financial services), although generally in favour of ensuring greater harmonisation across the MS, did not see a real need for lowering this amount and warned about the cost implications. Respondents belonging to certain professions (accountants, lawyers) also stressed the importance of clarifying the scope of the provision, and particularly the meaning of 'several operations which appear to be linked'.

---

116 The choice of a €7,500 threshold is explained by simply halving the existing threshold. 9 Member States currently apply thresholds below the existing €15,000 stipulated in the Directive, of which 4 Member States apply thresholds below €7,500. The expected impact on traders of a reduction of the threshold would not to increase costs, but rather to substantially reduce the number of transactions taking place using cash - to the advantage of other payment means (which may carry some additional costs – e.g. fees related to a credit card transaction). The impacts associated with the application of different thresholds (e.g. €10,000, €5,000) have (in the absence of available data) not been assessed, however it is reasonable to assume that they would not reveal significant differences with respect to the likely costs incurred by traders. There would however be different impacts on the number of cash payments, according to the chosen threshold.

Conclusion

There is a need to address vulnerabilities caused by different national approaches to ensuring that traders in high value goods apply CDD in appropriate circumstances. Reducing the threshold to conduct CDD to zero for certain specified traders may result in disproportionate costs. For that reason, the Commission has a preference for option 2, which is more proportionate to the Operational Objectives and would reduce the attractiveness of using the high value goods sector to launder the proceeds of robberies, while bringing greater convergence of approaches across Member States.

14. Strengthen the capacity of FIUs to cooperate across borders

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
Maintain current approach	0	0	0
	0	0	0
Strengthen FIU powers and cooperation by introducing new provisions in the Directive	+ Enhanced effectiveness of the fight against ML/TF + in line with Operational Objectives 1 and 2 + in line with Specific Objective 2	+ Enhanced legal clarity	+ Complements the EU's Internal Security Strategy
		- Some difficulties to exchange information may remain	
Establish a single European FIU	+ Enhanced effectiveness of the fight against ML/TF + in line with Operational Objectives	+ potential advantages in terms of economies of scale and efficiencies	+ Complements the EU's Internal Security Strategy
	- Requires substantial modifications to Member States' laws permitting cross-border cooperation and information sharing	- Potential additional costs at EU level	- Risk to delay agreement on the full package due to Member State concerns about sovereignty

Article 38 of the Third AMLD establishes a role for the Commission to facilitate coordination between FIUs, but does not otherwise deal with FIU cooperation.

The current framework for FIU Cooperation is based around a Council Decision dating back to 2000. However FIUs have complained that the current arrangements contain a number of shortcomings: cooperation on terrorist financing is not foreseen in the Decision and the recent past international events have brought to light difficulties for FIUs to cooperate on the basis of lists of designated persons, or to take action before an STR has been filed. Member States have different interpretations about the legal basis granted by the Decision to undertake specific types of cooperation, such as the automatic exchange of information when links are found with another Member State. Some of the problems in exchanging information stem from the different powers that FIUs have at national level, including the possibility to access information, and this has consequences for the effectiveness of cooperation.

Three options to strengthen cooperation are considered:

1. No change: this option would entail no additional costs. However deficiencies in cross-border cooperation would remain, and may constitute a factor of vulnerability in the AML/CFT framework.

2. Strengthen FIU powers and cooperation by introducing new provisions in the Directive: the FIU Platform has submitted a set of proposals aimed at enhancing cooperation, including providing an explicit legal basis for the matching of anonymous data between the EU FIUs or clarifying data protection rules to explicitly allowing certain types of information exchange: this option would not be especially costly to implement, and would serve to remedy the most significant problems encountered by FIUs. However it would be unlikely to overcome all the cooperation issues faced by FIUs.

3. Establish a single European FIU to receive and analyse and disseminate to the competent authorities disclosures of information from obliged entities operating within the EU: this option would require additional funds to be made available at EU level, and may raise concerns among Member States about sovereignty, and require quite far-reaching changes to Member States' rules and existing arrangements. However it would be more suited to an integrated EU financial market, and would also be arguably the most efficient and effective way to combat money laundering and terrorist financing across the EU, by allowing a more complete overview of the situation across the Internal Market. It would overcome the current cooperation difficulties which exist between national FIUs.

Stakeholders' views

Only a small number of respondents expressed a clear view on this issue. Of those that did, there was general support for the idea that effective co-operation and information sharing between FIUs across the EU was important and should be treated as a priority. Several respondents strongly supported inclusion into the Directive of the proposals discussed at the FIU platform. This support was however in some cases associated to the view that the Directive should not go beyond the international standards regarding international co-operation by calling for harmonisation, and that further experience of the impact of some new elements should be gained before going further in the harmonisation of powers at EU level.

Conclusion

The establishment of a single FIU would certainly be an efficient and cost effective means to ensure reception, analysis and dissemination of money laundering and terrorist financing reports in the Internal Market. However as it would require substantial modifications to Member States' legal frameworks and existing structures, and raise concerns about Member States' sovereignty, the Commission has a clear preference for option 2, which should nevertheless meet the operational objectives and result in increased effectiveness in the fight against ML/TF.

ANNEX IV: COSTS OF COMPLIANCE WITH THE THIRD AMLD BY CROSS-BORDER BANKING GROUPS AT GROUP LEVEL (EXTRACT FROM THE COMMISSION STAFF WORKING DOCUMENT SEC(2009) 939 FINAL)

The cost of compliance with AML requirements is not insignificant and has increased in recent years following the regulatory changes introduced in the EU, notably the AML Directive[117].

A recent external study has examined for the Commission the cost impact of compliance for certain types of firms within the financial industry (including banks) with six key EU directives in the financial services area, including the AML Directive[118]. The study focuses on the so-called 'incremental compliance costs' caused by regulation, not on the total costs of activities that happens to contribute to regulatory compliance[119].

The study separately identifies cost impacts that are of a one-off nature (i.e. those costs that only have to be incurred once in making the transition, such as IT investment and the re-shaping of business processes) from those that are recurring in nature (i.e. on-going costs as a result of regulation). The ongoing costs of compliance for any given firm are typically lower than the one-off costs. Looking at the different sectors surveyed, recurring costs are mostly between 15 and 20 per cent of the implementation cost recorded (with some exceptions)[120]. Figure IV.1 illustrates this divergence in scale, by showing the dispersion of the results obtained for the AML Directive.

This study shows that firms have adopted different strategies in approaching the implementation of the Directive, both regarding one-off (in particular, in their willingness to put maximum reliance upon the automation of processes) and ongoing costs. The dispersion of the ongoing costs — and general business experience — suggest that firms have experienced mixed results in terms of their success in achieving this objective. Indeed the study shows a wide dispersion of results.

---

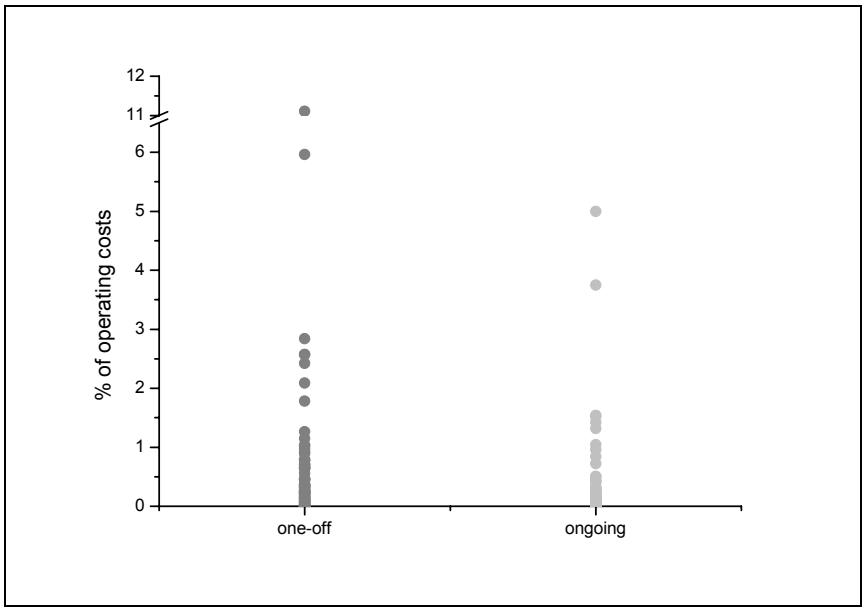
117 See CRA International (2009), p.13. According to the KPMG survey of 2007, a range of European banks estimated that their AML compliance costs increased by 58% over the 2004-2007 period. This survey also predicts that costs will grow at a slower rate in the following years: indeed European banks expect these costs to increase by 27% between 2007 and 2010. This survey underlines the difficulty of estimating AML costs as they may be spread across many different functions (operations, compliance, risk) or regions, involve direct and indirect costs, and overlap with processes that are embedded in normal business practice (e.g. credit risk or customer relationship management). This survey does not make a distinction between one-off and on-going costs of compliance. See KPMG (2007), p.14 and seq.

118 Europe Economics (2009). The survey concentrated on firms from four sectors within the financial services industry in the EU: banks and financial conglomerates, asset managers, investment banks and financial markets. The six directives concerned are the so-called Prospectus Directive, the Financial Conglomerates Directive, the Capital Requirements Directive, the Transparency Directive, the Markets in Financial Instruments Directive – MiFID and the AML Directive. These measures were part of the Commission's Financial Services Action Plan (FSAP) of 1999 (the so-called 3rd AML Directive of 2005 replaced in the meantime the precedent, second, AML Directive of 2001 which was the measure addressed in the FSAP).

119 *Ibid*., §2.14. For an explanation of the methodology of this study, see: section 2; the introductions to sections 4 and 5; as well as Appendix 1 of the final report.

120 *Ibid*., §15 and seq..

Figure IV.1: Dispersion of one-off and ongoing costs of the AML Directive (expressed as a percentage of 2007 operating expenses)



Source: Europe Economics (2009), figure 3.

TABLE IV.1 – AML Directive – One-off costs of compliance[121]

	Banks & financial conglomerates	Investment banks	Asset managers	Financial markets
Mean[122] (percentage of 2007 operating expenses)	0.29%	0.23%	0.21%	0.16%
Median[123] (percentage of 2007 operating expenses)	0.31%	0.32%	0.24%	0.03%
Total financial services regulatory compliance costs[124] (percentage of 2007 operating expenses)	2.90%	2.25%	1.58%	3.40%
Mean: average absolute value of the incremental cost changes, per firm (€000s)	4,588	2,507	825	33
Total financial services regulatory compliance costs (€000s)	45,149	24,569	5,565	694
Average of operating costs (€000s)	1,558,072	1,030,071	384,582	20,403

121 Source: Europe Economics (2009), tables 4.1, 4.2 and 4.3.

122 The middle value in a series of data points arranged sequentially. The sequence from which this median has been selected is based upon the estimated one-off costs of compliance expressed as a percentage of the relevant firm's more recent operating expenditure.

A) The one-off costs of compliance

With respect to one-off costs of compliance (see Table IV.1) for banks, financial conglomerates and investment banks, compliance with the AML Directive roughly accounts for 10% of all their financial services regulatory costs.

The difference in costs between banks and financial conglomerates on the one hand, and investment banks, on the other, may be due to the typically different client make-up[125]. The study also notes that in the AML field, firms voluntarily practice standards that are applied globally, which adds to the costs resulting from the Third AMLD[126]. If a comparison is made with the costs of compliance for asset managers, Table IV.1 shows that the one-off costs of compliance with the Third AMLD assume a higher proportion of asset managers' total costs[127].

Out of the six Directives examined in the study, the Third AMLD ranks third in terms of cost impact for banks, financial conglomerates and investment banks, behind the Capital Requirements Directive and MiFID. These two other Directives represented the most important regulatory changes in this area in recent times and their compliance costs are significantly higher[128]. The study identifies the possibility for firms to achieve synergies between some of the requirements in the AML Directive and MiFID: a small number of institutions surveyed felt that synergies had been achieved (or could be achieved) between the "know-your-customer" requirements of the AML Directive and suitability tests of MiFID[129]. Nevertheless, very few businesses believed that any significant cost-reducing synergies had been achieved in the implementation of the various measures: the variation in the implementation dates was the most frequently cited factor behind this. Another component to this problem was that firms felt that the detail necessary to properly prepare for IT changes was not always forthcoming from the implementing authorities in a sufficiently timely manner.

---

123 Aggregate one-off costs of compliance expressed as a percentage of the relevant firms' aggregated most recent operating expenditure. This implies that the experience of the larger firms will carry more weight in the sample presented.

124 Including other FSAP measures and other financial services regulation, whether EU, nationally or extra-territorially derived.

125 *Ibid*., §4.10. The study also provides further breakdowns of costs, per size and geographical origin. See §4.20 to 4.25 and 4.93 to 4.94.

126 *Ibid*., §4.12 in fine. The non-EU regulation costs are reflected in the study, on an aggregated basis, in the total costs.

127 Financial markets (e.g. stock exchanges operators) are not directly subject to the obligations of the AML Directive. But in order to allow for comparisons, their costs are also shown in Table IV.1.

128 *Ibid*., tables 4.1, 4.2 and 4.3. The impact of MiFID costs doubles those of the AML Directive, while CRD accounts for more than half of the total financial services regulatory compliance.

129 *Ibid*., §§4.14 to 4.17. This is also confirmed by the KPMG survey of 2007. See KPMG (2007), p.53.

The main source of Third AMLD-related compliance spending is on IT (see Table IV.2 for banks and financial conglomerates and Table IV.3 for investment banks).[130] Similarly high IT costs appear for almost all the Directives covered.

TABLE IV.2 – Cost drivers of the selected directives (banks and financial conglomerates) – one-off costs

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Familiarisation with Directive	49%	15%	2%	13%	3%	3%
Consultancy fees	5%	11%	20%	5%	13%	11%
Legal advice	23%	5%	5%	5%	7%	1%
Training	13%	8%	5%	11%	15%	22%
Staff recruitment costs	0%	2%	4%	1%	2%	2%
Investment in/updating IT	2%	47%	57%	63%	52%	54%
Project management	8%	9%	8%	3%	7%	7%
Other	0%	2%	0%	0%	0%	0%

Source: Europe Economics (2009), table 4.10.

TABLE IV.3 – Cost drivers of the selected directives (investment banks) – one-off costs

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Familiarisation with Directive	9%	7%	3%	7%	6%	5%
Consultancy fees	13%	0%	19%	10%	16%	12%
Legal advice	18%	10%	2%	4%	4%	6%
Training	14%	15%	2%	4%	10%	13%
Staff recruitment costs	4%	0%	1%	10%	1%	0%
Investment/ updating IT	27%	39%	62%	36%	49%	53%
Project management	14%	29%	10%	29%	14%	12%
Other	0%	0%	1%	0%	1%	0%

Source: Europe Economics (2009), table 4.27.

In terms of IT spending[131], this included projects designed to: (i) meet the "Know-Your-Customer" informational requirements, such as some adaptation of the existing Customer Relationship Management systems and/or some new data entry needed to meet these increased data capture requirements (in a few instances, this triggered data warehousing projects to enhance inter-system data capture); (ii) facilitate increased monitoring of suspicious transactions through increased automation of processes[132]; (iii) facilitate Politically Exposed Persons screening; and (iv) assist in risk assessment.

Training and (for larger banks) external consultants are also important sources of cost. According to the study, the importance of training in the AML field is driven by it being more generally applicable than for the other Directives: in other words, the breadth of coverage of

130 See generally, *Ibid*., §§4.57 to 4.62, and §§4.106 to 4.107.

131 *Ibid*., §§4.58 and 4.59.

132 A different survey carried out in 2007 by a consultancy firm found that transaction monitoring is the single greatest area of AML expenditure for banks. See KPMG (2007), p.16 and 33.

the training believed to be necessary to comply with this measure was greater than for the others. There were also some costs associated with the re-design of training programmes and the roll-out of these[133].

These findings are fundamentally the same as those from a different (and qualitative) survey conducted in 2007. According to that survey, the drivers of higher expenditure in the 2004-2007 period appeared to be greater expenditure on transaction monitoring capabilities and upgrades to existing systems, and the provision of additional tailored training to staff (in that survey there was no distinction between one-off and on-going costs).[134]

The study notes that the implementation of the AML Directive remains a work-in-progress. Trans-national businesses have typically implemented their provisions on a group basis, either using the Directive itself as guidance or the implementation in their own Member State (if it had been implemented). Their expectation is, however, that additional expenditure will be necessary in the future to adapt to the requirements of the local transposition. Some participants argued that the uneven transposition situation represented a disincentive to early adoption[135].

B) The ongoing cost of compliance

Concerning the ongoing cost of compliance (see Table IV.4) for banks, financial conglomerates and investment banks, compliance with the Third AMLD roughly accounts for 13% of all their financial services regulatory costs[136]. In relative terms, this is a slightly higher figure than the one-off cost of compliance, possibly explained by the relatively lower on-going costs of compliance with the Capital Requirements Directive and MiFID. In any event, as for the one-off costs, these two other Directives take up the bulk of the compliance costs, with the AML Directive ranking third out of the six Directives examined by the study. If a comparison is made with the ongoing cost of compliance for asset managers, Table IV.4 shows that the ongoing cost of compliance with the AML Directive assumes a lower proportion of asset managers' total costs, which is explained by the higher ongoing cost incurred by asset managers regarding MiFID and Prospectus Directive[137].

TABLE IV.4 – AML Directive – Ongoing cost of compliance

	Banks & financial conglomerates	Investment banks	Asset managers	Financial markets

133 Europe Economics (2009), §§4.57 and 4.60.

134 Respondent banks estimated the areas of greatest AML expenditure according to the following categories (the ranking is based on a maximum score of 5 for 'very strong impact' and a minimum score of 1 for 'no impact'): enhanced transaction monitoring (4.1); greater provision of training (3.4); sanctions compliance (3.4); remediation of KYC documentation for existing customers (3.3); transaction 'look-bank' reviews (3.2); increased external reporting requirements 3.2); introduction of global procedures (3.0); more complex account-opening procedure (3.0); and increased internal reporting requirements (2.8). See KMPG (2007), p.16.

135 Europe Economics (2009), §4.62.

136 The study also provides further breakdowns of costs, per size and geographical origin. See §§5.12 to 5.17 and 5.62.

137 Financial markets (e.g. stock exchanges operators) are not directly subject to the obligations of the AML Directive. But in order to allow for comparisons, their costs are also shown in Table IV.4.

Mean[138] (percentage of 2007 operating expenses)	0.08%	0.05%	0.07%	0.13%
Median[139] (percentage of 2007 operating expenses)	0.09%	0.08%	0.07%	0.00%
Total financial services regulatory compliance costs[140] (percentage of 2007 operating expenses)	0.59%	0.38%	0.85%	1.70%
Mean: average absolute value of the ongoing costs incurred, per firm (€000s)	1,195	464	278	27
Total financial services regulatory compliance costs (€000s)	8,540	3,807	2,532	347
Average of operating costs (€000s)	1,558,072	1,030,071	384,582	20,403

Source: Europe Economics (2009), tables 5.1, 5.2 and 5.3.

The most important ongoing costs of compliance associated with the Third AMLD concern IT expenditure and additional staff costs (see Table IV.5 for banks and financial conglomerates and Table IV.6 for investment banks).[141] Most of the IT expenditure is linked to access costs to various databases dedicated to the tracking and screening of relevant parties such as Politically Exposed Persons, watch lists etc. Whilst some firms (generally larger banks) see automation as the only way to provide the necessary evidence of an audit trail to the regulatory authorities in the event of problems arising (as well as being cost effective by comparison to manual effort), a number of firms have retained significant (or total) human oversight in this area.

TABLE IV.5 – Cost drivers of the selected directives (banks and financial conglomerates) – ongoing cost

	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Additional staff	37%	6%	43%	15%	35%	37%
Internal reporting	2%	7%	8%	4%	7%	4%
IT	15%	6%	26%	49%	28%	31%
External reporting	16%	65%	10%	8%	10%	5%
Training	19%	4%	6%	8%	10%	13%
Audit	10%	11%	7%	15%	9%	10%
Other	0%	0%	0%	0%	0%	0%

Source: Europe Economics (2009), table 5.10.

TABLE IV.6 – Cost drivers of the selected directives (investment banks) – ongoing cost

138 The middle value in a series of data points arranged sequentially. The sequence from which this median has been selected is based upon the estimated ongoing costs of compliance expressed as a percentage of the relevant firm's more recent operating expenditure.

139 Aggregate ongoing costs of compliance expressed as a percentage of the relevant firms' aggregated most recent annual operating expenditure. This implies that the experience of the larger firms will carry more weight in the sample presented.

140 Including other FSAP measures and other financial services regulation, whether EU, nationally or extra-territorially derived.

141 See generally, *Ibid*., §§5.34 to 5.40 and §5.69.

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Additional staff	0%	0%	34%	33%	26%	23%
Internal reporting	0%	23%	7%	7%	6%	12%
IT	1%	35%	32%	19%	45%	29%
External reporting	48%	12%	10%	8%	13%	9%
Training	47%	31%	6%	12%	6%	16%
Monitoring/audit	3%	0%	10%	21%	4%	10%
Other	0%	0%	0%	0%	0%	0%

Source: Europe Economics (2009), table 5.27.

Ongoing training is not an insignificant cost factor. However, it the study points out that once e-learning or class-based training modules have been developed (see one-off costs), the ongoing requirements in cost terms is mitigated[142]. It is also noted that whereas large banks spent proportionately more than small banks on training as a one-off cost, the proportion of training within ongoing costs is lower. This would be consistent with larger banks being more reliant on e-learning and e-training.[143]

142 Interviewees in the study were not in agreement as to whether the AML Directive increased the intensity of training required — i.e. whether or not the duration of the training sessions increased or were rolled out to a broader set of employees. See *Ibid*. §5.36.

143 Some participants remain sceptical about e-learning generally. It is seen by such firms as a "quick fix", in essence allowing maximum access to training for more people in less time. However, these firms considered it inevitable that it would require supplementation by more traditional (and more expensive) classroom-based approaches. See *Ibid*. §§5.37 and 5.38.

ANNEX V: SECTOR BY SECTOR ANALYSIS OF IMPACTS

V.1. THE BANKING SECTOR

General description of the Sector

The European Banking Sector is the largest in the world with over 6,800 institutions, over three million employees and total assets of over 40 trillion EUR. The total number of bank employees amounted to 3.2m[144]. In 2010, the total number of non-cash payments in the EU increased by 4.4% to 86.4 billion, of which card payments accounted for 39% of all transactions, while credit transfers accounted for 28% and direct debits for 25%[145].

Compliance costs

Over the past years financial institutions made important investments to set up compliance departments and procedures to fight against money laundering and terrorism financing. One large EU bank, with several hundred thousand employees estimated that around 10% of its workforce was involved (fully or partially) in AML compliance work.

Money Laundering in the Banking Sector (US)[146]

In March 2010, a US bank, Wachovia, settled the biggest action yet brought under the US bank secrecy act. In published court documents, across-the-board failings were identified in the bank's AML system.

Over the course of 2004-2007, Wachovia conducted transactions with Mexican currency exchange houses (CDC's), allowing them to wire transfer funds through accounts at Wachovia to recipients throughout the world. According to the court documents, Wachovia did not have an effective anti-money laundering policy or procedure to monitor these transactions to detect and report potential money laundering activity. From May 2004 to May 2007, at least $373 billion in wire transfers were made from the Mexican currency exchange houses to Wachovia accounts; more than $4 billion in bulk cash was transported from the CDCs in Mexico to accounts at Wachovia; and approximately $47 billion was deposited at Wachovia accounts through a "remote deposit capture" service. These monies included millions of dollars that were subsequently used to purchase airplanes for narcotics trafficking operations. Ultimately, more than 20,000 kilograms of cocaine were seized from these airplanes.

According to the information and other documents filed with the court, Wachovia failed to effectively monitor for potential money laundering activity more than $420 billion in financial transactions with the CDCs.

144 Statistics on Consolidated Banking Data, European Central Bank, reference end-June 2011 and end-June 2010

145 Source: "EU Banking Sector: The world's largest banking system in the world's largest economic space. Facts and Figures 2011/2012, European Banking ", European Banking Federation.

146 Source: The United States Attorney's Office, Southern District of Florida, Press Release, March 17th 2010

The bank was sanctioned for failing to apply the proper anti-laundering strictures and paid federal authorities $110m in forfeiture, for allowing transactions later proved to be connected to drug smuggling, and incurred a $50m fine for failing to monitor cash used to ship 22 tons of cocaine.

V.2. THE PAYMENTS SECTOR

General description of the Sector

The total number of credit institutions and payment institutions in the EU offering payment services to non-monetary financial institutions in 2010 amounted to 8,604[147].

Compliance costs

One Payment Institution has provided estimates for the cost applicable to Compliance/AML functions. It has a total headcount of 238 persons dedicated to Compliance/AML functions. This does not include headcount relating to other departments that closely support the Compliance/AML function, e.g. the Legal and Regulatory Affairs departments. The total headcount of this Payment Institution's group is just over 2400, and therefore Compliance/AML represents approximately 10% of the company's total headcount.

Additionally, other costs can be attributed to the running of our Compliance/AML function, e.g. the cost of external consultants, the cost of real estate to cater for the Compliance/AML personnel, IT costs relating to specific software/hardware needed for compliance reasons (e.g. use of external databases to verify customers' ID).

Terrorist Financing in the Payments Sector (Belgium - Informal Money remittance System)

An East African residing in Belgium, Mr X, stated that he performed Hawilaad banking activities. His account was exclusively credited by cash deposits and numerous transfers in small amounts. During several months the funds were transferred to company A in Eastern Africa. Shortly afterwards the funds were transferred to company B in Western Europe. Companies A and B performed money remittance transactions around the globe. Mr X claimed that he performed Hawilaad activities for fellow countrymen wishing to send money to Eastern Africa. However, he did not hold any position within Belgian companies and he was not registered as manager of an authorised exchange office. The individual did not have an authorisation from the CBFA (banking supervisor) either. Police sources revealed that he was known to be a member of a terrorist organisation. In this case the alternative remittance system may have been used for terrorism financing.

Money Laundering through money transmitters (France)

An individual "A" residing in an Eastern Europe country received hundreds of funds transfers usually in small amounts through a money remitter service provider initiated by more than 35 women of the same nationality as individual A. Typically the number of remittances initiated by each person was small (four on average). The addresses disclosed by the women referred to different hotels situated in Paris. Most of the women did not have a criminal record and did

147 Source: European Central Bank, Payments statistics - INSTITUTIONS OFFERING PAYMENT SERVICES TO NON-MFIS

not hold a bank account. One of the women however had opened bank account in France and indicated as her address the address of a company whose manager was convicted for aggravated procurement some years ago.

The case was transmitted by Tracfin (the French FIU) to the judicial authorities on a presumption of involvement in the procurement of prostitutes.

Source: Money Laundering through Money Remittance and Currency Exchange Providers – 2010 2011 Moneyval and FATF/OECD

V.3. THE E-MONEY SECTOR

General description of the Sector

E-Money can be issued by licenced credit or financial institutions, or else by specialist licenced E-Money institutions, of which there are currently around 35 such institutions operating under the EU E-money licence[148]. Throughout the EU in 2010, total number of e-money purchase transactions stood at just over 1 billion, accounting for 1.2% of the total number of transactions[149].

The e-money product first introduced and in use is the **'electronic purse'**, which allows users to store relatively small amounts of money on a payment card or other smart card, to use for making small payments. E-money can also be stored on (and used via) mobile phones or in a payment account on the internet. In the latter case, funds are stored on a central server (e.g. at the provider) and are often used in pre-funded personalised online payment schemes, involving the transfer of funds stored on a personalised online account (not including traditional bank deposits). The best-known example of these services is **PayPal**. The advantage for consumers is that it allows them to purchase in a secure way on the internet without disclosing credit card details. Another increasingly popular e-money product is based on prepaid cards which are not linked to a bank account, but instead often used in conjunction with online accounts for purposes such as e-gambling. Card issuers using the MasterCard brand alone provide 11 million prepaid cards in the EU.[150]

Compliance costs

Compliance costs will vary considerably according to each business model, and the Commission has received no publishable data in this respect.

Given the often low value involved in payment transactions, some representatives of the E-Money industry have expressed concerns about changes which would entail a need to conduct due diligence measures at an early stage in the relationship with the customer. The current simplified regime in the Third AMLD allows Member States to not require application of CDD in the case of E-money where a non-rechargeable device where the maximum stored value is €250, or in the case of rechargeable devices until a limit of €2,500.

148 According to the E-Money Association

149 Source: European Central Bank - payment and terminal transactions involving non-MFIs, total number of transactions: 5. E-money purchase transactions

150 Information retrieved from MasterCard comments to the Commission on the Third AML Directive.

Money Laundering in the E-Money Sector

Many New Payment Methods rely on a business model where face-to-face customer contact is minimal or non-existent. This can facilitate abuse by criminals for money laundering purposes.

In some cases some shortcomings in some providers´ identification and verification processes and monitoring systems is likely to have contributed to the illegal activity going undetected for some time.

Laundering of phishing activity proceeds through prepaid cards (Italy)

In this case, prepaid cards are used as transit accounts where criminals sent funds from bank accounts after identity theft of the accounts' holders. The phisher pretended to be the bank account holder and sent funds to the prepaid card that was issued in the name of a strawman. After the funds were transferred to the card, a corresponding amount of cash was withdrawn at ATMs.

Laundering of counterfeiting and fraud proceeds through open-loop prepaid cards (Belgium)

Within a few months, the accounts of Mr. POL and company BE were credited by international transfers for some € 500 000 from a Swiss company acting as an agent and trader in securities. These funds were used to load prepaid cards. In most cases, these cards were loaded with € 5 000 (maximum limit). Mr. POL claimed to have loaded these prepaid cards because he had given them to his staff for professional expenses. As soon as the money was loaded on the cards, the card holder quickly withdrew the money by repeatedly withdrawing cash from ATM machines.

Mr. POL was the subject of a judicial investigation regarding counterfeiting and fraud. Given the police information on Mr. POL, the funds from Switzerland may have been of illegal origin and linked to the fraud and counterfeiting for which Mr. POL was known. This hypothesis was confirmed by the ingenious scheme (international transfers, prepaid cards and cash withdrawals) used to repatriate funds to Belgium.

Source: FATF report: Money Laundering Using New Payment Methods October 2010

V.4. ACCOUNTANTS AND EXTERNAL AUDITORS

General description of the Sector

With respect to external accountants, a recent survey carried out by FEE , the national professional institutes of accountants and auditors across 30 European countries (27 EU Member States plus Croatia, Iceland and Norway) quantified total membership at around 700.000 members. Some of these members also provide tax advice.

Professional accountants provide a wide range of - sometimes mutually exclusive - services, including preparation of financial information, tax services, statutory audit, as well as many innovative services in the areas of non-financial reporting, assurance services other than statutory audit, sustainability and corporate social responsibility, strategy and management consultancy and corporate governance.

With respect to the **audit profession**, there are estimated to be over 230,000 approved statutory auditors and audit firms in the EU[151].

Compliance costs

One large UK-based accountancy firm has estimated AML compliance costs as follows:

The compliance team consists of an equity partner (30-50 % of their time), a director (full-time) a senior manager and 5 other assistants. In addition, a team of around 100 other staff work in back office compliance.

Web based training courses cost c£100,000 which is cost effective for around 15,000-16,000 staff.

Customer Due Diligence checks take around 0.5 – 1 hour for a "normal" client, and up to a day or 2 even days for more complex corporate/trust clients.

Source – meeting report with the Accountancy sector.

Money Laundering involving accountants and tax advisors (The Netherlands)

The Tax Administration and the Fiscal Intelligence and Investigation Service discovered activities involving the allocation of securities as a means to effect tax fraud. These activities involved the use of false documents, in violation of tax and criminal laws. The cases involved different players in the financial sector; involving employees of financial institutions along with accountants and tax advisors.

The cases investigated have in common the misuse of a normal and legitimate service provided by banks, broker-dealers and other institutions licensed to trade in securities: the ability to transfer securities held electronically.

The misuse in the Dutch cases was triggered by a difference in the way capital gains and losses were treated for the income and corporate tax purposes. In short, capital losses are not deductible for income tax purposes, but are included in the tax base for corporate tax. Individuals transferred securities between their personal portfolio and a corporate securities portfolio over which they had control. Depending on what was necessary in the specific case, securities were transferred in either direction. In the case of a loss that occurred in the personal portfolio, the relevant securities were transferred to the corporate stock portfolio and vice versa.

Source: Money laundering and terrorist financing in the securities sector October 2009 FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf

V.5. THE INSURANCE SECTOR

General description of the Sector

151 European Commission, impact assessment accompanying the proposal for a Directive amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts: Annex 3 –Approved statutory auditors and audit firms, SEC(2011) 1384 final.

In the insurance sector, total life insurance premiums end 2010 amounted to €676 billion; there were over 5000 insurance companies (end 2010) and close to one million employees working in the insurance sector (life + non-life combined).

Compliance costs

In general, insurance firms need to make large investments in order to comply with the AML rules. Insurance Europe has provided the following estimates for the current cost of compliance in several markets:

- The Association of British Insurers estimates the current cost of compliance of one of its members. In terms of **staffing**, annual costs for 6 full time equivalent posts are estimated at £400,000 per annum. An additional 55 people who devote part of their time to active AML controls are estimated at £250,000 per annum. In addition, **automated electronic controls** instigated over the past 4 years cost an additional £6m.

- Most insurers have made investments in **automatic detection systems** (recommended at least for larger insurers in Belgium by the Belgian supervisory authority). In addition, insurers are also obliged to (continuously) **train** their employees on the risks of money laundering through insurance. The more fundamentally the system changes the more costs the insurers will incur as they will be obliged to update their whole system, their training programmes for employees etc.

- For the Netherlands, the following cost indications were provided:

    - ABZ is an **IT supplier** in the Dutch insurance sector: the higher the number of records that have to be dealt with by ABZ, the higher the category of costs ABZ will charge. Categories vary from 1 to 10. One Dutch insurer has 20 million records in total which need to be checked 6 times per year (a requirement of the Dutch Supervisor). Consequently this means that 120 million records need to be checked per year, for which ABZ will charge according to category 10: costs of such an audit will reach € 100,000. In addition to these costs, costs for licenses per user/business and cost of the PEP list will be also charged.

    - The **estimated increase in online checking costs** would be € 500,000 to 1,000,000. Furthermore, internal handling costs for PEP reports from inspections are estimated at 16,000 reports per year (assuming 10% of the PEP-list which consists of 160,000 PEPs) and continuous monitoring (estimate 3 for three full time employees = 3 x 50,000 = € 150,000).

Insurance Europe has indicated that in many EU countries, the current AML regime for the insurance sector has resulted in higher costs in terms of resources, unnecessary and inefficient use of resources, and which did not appear helpful in terms of law enforcement. They argue that resources should have been best used and applied only to those products that actually present a risk for ML/TF.

However Insurance Europe also believes that the expansion of the RBA across all anti-money laundering areas will result in a sound and logical asset and resource allocation to those areas where the real risk of money laundering exists. This could be a real improvement, especially with regard to very labour intensive measures such as identification of beneficial owners or Politically Exposed Persons (PEPs). The RBA enables companies to focus ML compliance resources where there is the greatest ability to be helpful to law enforcement, provided there is a strong requirement that insurance companies have completed and documented a detailed ML risk assessment of their own products and business.

Money Laundering through the Insurance sector (Bulgaria)

A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr A by Mr A's employer, who was a related person.

Half of the amount was withdrawn by Mr A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time.

In follow-up to a report to the FIU, checks revealed that Mr A had a criminal record and was involved in pending legal proceedings. It also emerged that Mr A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, CTRs, and movements of funds on Mr. A's accounts the relevant information was forwarded to law enforcement agencies.

Source: Typology research: Money laundering through private pension funds and the insurance sector – October 2010.

http://www.coe.int/t/dghl/monitoring/moneyval/typologies/MONEYVAL(2010)9_Reptyp_full_en.pdf

V.6. LAWYERS/NOTARIES

General description of the Sector

With respect to **notaries**, the total number in the EU is estimated to be around 38,500[152].

With respect to the number of **independent legal professionals**, the total number is estimated to be around 900,000 (2008)[153].

Compliance costs

Representatives of the legal and notary professions have indicated that cost of compliance with AML/CFT rules is a key concern.

- Notaries have indicated that the principal costs of compliance stem from technology (building systems) and external costs (such as subscribing to PEPs databases).

152 Source: Notaires d'Europe

153 Council of Bars and Law Societies of Europe, CCBE Brochure 2010, *Nombre d'avocats dans les pays membres 2008*.

- Lawyers have in particular highlighted the time cost in dealing with compliance issues, with what is perceived as little added value for AML, as the vast majority of their cases are lower risk.

Representatives of both professions have felt that the burden falls more greatly on small businesses, although they did not disagree that smaller firms do not necessarily always have lower risk clients[154].

Money Laundering involving a Lawyer (Spain)

A lawyer created several companies on the same day (with ownership through bearer shares, in order to conceal the identity of the true owners). One of these companies acquired a property that was an area of undeveloped land. A few weeks later, the area was re-classified by the town hall where it was located so that it could be urbanised.

In successive operations at the Property Registry, the lawyer transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions.

With each successive transfer of the property, the price of the land was increased. The participants in the individual transfers were shell companies – also controlled by the lawyer. Finally the mortgage was cancelled through payment by cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as the acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it could be concluded that this company was a front company set up merely for the purpose of carrying out the property transactions.

After further investigation, it emerged that the purchaser and the seller were one and the same person: the leader of a criminal organisation. The money used in the transaction had illicit origins (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Source: ML/TF through the real state sector FATF June 2007

http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf

V.7. THE GAMBLING SECTOR

General description of the Sector

The overall size of the gambling market, measured in terms of "Gross Gaming Revenues" (i.e. stakes minus winnings) is equal to €71.9 bln (off-line) and €8.5 bln (on-line) in 2010. The market share of on-line business is growing rapidly.

154 Source - meeting report with lawyers and notaries on 24 May 2012

With respect to Casinos, there were an estimated 800 casinos operating in the EU, employing 60,000 staff. Lotteries employ 19,000 staff, while the gaming and amusement machines and devices sector (not casinos) employ 245,000 staff.

Compliance costs

The European Casino Association (ECA) have provided individual anonymous data for compliance costs under the Third AMLD for two casinos (Casino A and Casino B)[155]:

Types of costs	Casino 1	Casino 2
Training / involvement – upper management	€ 7,200	€ 28,800
Legal consultancy	€ 8,000	€ 40,000
AML/CFT advice from external consultants	€ 4,000	
Auditing	€ 5,000	€ 6,000
Regulation costs		€ 11,000
Depreciation systems		€ 65,000
Fees for third parties (use of databases)[12]	€ 5,000	€ 38,000
AML/CFT project-steering team	€ 14,400	€ 38,000
Training – 'on the floor' staff, meetings	€ 8,750	€ 287,600
Daily duties on the floor: internal and external reporting, observation, information seeking, exchange of information, conversations with customers, administration, etc	€ 65,700	€ 524,000
Total costs per casino per year:	**€ 118,050**	**€ 1,038,400**

Money Laundering Typology in the gambling sector

Money laundering in a Casino (UK)

One money laundering conspiracy involved millions of UK pounds from organised criminal gangs being laundered by a group of men from West Midlands. The money laundered included the profits from a number of activities including drug trafficking, multi-million pound VAT conspiracies in the mobile phone industry, counterfeiting and credit card fraud. The monies were a mixture of Scottish and English notes. The defendants would transfer large amounts of money to a back account in Dubai, which would then be accessed by their associates. The defendants received the proceeds of crime in the UK and made equivalent amounts of criminal monies available in Dubai. They then utilised the gambling industry to launder the money. Money was placed on a deposit at a casino and withdrawn a day or so later. Other sums would be gambled. Thousands of pounds would be passed over the tables in order to disguise the original source of the banknotes. Monies gambled or exchanged at the casino provided the defendants with an apparently legitimate explanation as to their source.

Source: FATF report: Vulnerabilities of casinos and gaming sector (March 2009)

155 Source European Casino Association response to the European Commission questions relating to the review of the third Anti Money Laundering Directive, 3 October 2011.

V.8. REAL ESTATE SECTOR

General description of the Sector

The total number of **real estate agents** has been quantified by Eurostat at 1.3 million enterprises and 3.3 million employees (2009)[156].

Money Laundering in the Real Estate Sector ("THE WHITE WHALE CASE")[157]

In Spain, drug-trafficking proceeds were laundered through a scheme involving shell companies and investments in the real estate sector. Beneficial ownership was kept hidden and notaries and lawyers were misused. Despite the fact that there were suspicions of money laundering (incorporation of several companies by the same persons within a short period of time, same partners in several companies, several real estate purchases in a short period of time, etc.) and although public notaries were obliged to report under the Spanish anti-money laundering law, transactions were not disclosed to the Spanish FIU

The launderer transferred funds from a foreign country to a non-resident account owned by a Spanish company. The funds were pooled in the account of the Spanish company under the guise of foreign loans received. At the final stage of the process, the funds were used to purchase real estate properties in the name of the Spanish company, with the identity of the money launderer and the beneficial owners remaining hidden.

The off-shore companies involved in this case were "shell companies" established in a US State whose laws allow a special tax regime for such companies and for their transactions. The companies were pre-constituted in the name of an agent (usually a lawyer) before the incorporation of the company, with the document of incorporation of the company remaining inactive in the hands of the agent until the company was purchased by a client.

The total amount of money laundering from drug trafficking and prostitution was estimated at €250 million.

Source: FATF report: The misuse of corporate vehicles, including trust and company service providers (2006)

156 Source: Eurostat, Real estate, renting and leasing statistics - NACE Rev. 1.1, 2009 data

157 Source: FATF report: The misuse of corporate vehicles, including trust and company service providers (2006)

ANNEX VI: MEMBERSHIP OF FATF AND MONEYVAL

The Financial Action Task Force – the standard setter for international AML/CFT rules

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary consensus to bring about national legislative and regulatory reforms in these areas. 15 EU Member States[158], as well as the European Commission, are full members of FATF.

Membership

Argentina	Australia	Austria	Belgium
Brazil	Canada	China	Denmark
European Commission	Finland	France	Germany
Greece	Gulf Co-operation Council	Hong Kong, China	Iceland
India	Ireland	Italy	Japan
Republic of Korea	Luxembourg	Mexico	Netherlands, Kingdom of
New Zealand	Norway	Portugal	Russian Federation
Singapore	South Africa	Spain	Sweden
Switzerland	Turkey	United Kingdom	United States

158 BE, DK, DE, GR, ES, FR, IE, IT, LU, NL, AT, PT, FI, SE, UK

Moneyval[159] – the Committee of Experts on the Evaluation of Anti-money Laundering Measures and Financing of Terrorism

The aim of Moneyval is to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields. Moneyval currently comprises 30 members which are subject to its evaluation processes and procedures, including 12[160] EU Member States which are not members of FATF.

Membership

Albania	Andorra	Armenia	Azerbaijan
Bosnia and Herzegovina	Bulgaria	Croatia	Cyprus
Czech Republic	Estonia	Georgia	Hungary
Holy See (since April 2011)	Israel (since January 2006)	Latvia	Liechtenstein
Lithuania	Malta	Moldova	Monaco
Montenegro	Poland	Romania	Russian Federation (also FATF member since 2003)
San Marino	Serbia	Slovak Republic	Slovenia
"The former Yugoslav Republic of Macedonia"	Ukraine		

159 Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

160 BG, CZ, EE, CY, LV, LT, HU, MT, PL, RO, SI, SK

ANNEX VII: EFFORTS TO MEASURE EFFECTIVENESS OF AML MEASURES BY THE COMMISSION

Important first steps to measuring the effectiveness of AML measures through the establishment of a set of indicators have been taken by DG HOME and EUROSTAT, in recognition of the need to develop better statistical knowledge at national and European level and to provide a more precise and reliable diagnosis of the criminal threat. "**Money Laundering in Europe**"[161] is one of the fruits of a 2006-2010 action plan entitled "Developing a comprehensive and coherent EU strategy to measure crime and criminal justice". The publication represents a first step towards enabling a cost/benefit analysis of anti-money laundering provisions, which would feed into and clarify not only political decision-making, but also operational cooperation.

While recognising the limitations - resulting from the different approaches and set-ups at national level for the combat against money laundering – of making cross-country comparisons, the report paints a useful picture of Member States' efforts in this field. The report contains data on the number of suspicious transaction reports (STRs) filed, according to each category of obliged entity, how many reports were sent to law enforcement, how many staff are dedicated to full-time AML work within FIUs, how many cases were initiated by law enforcement agencies on the basis of STRs received, the number of cases brought to prosecution, the number of persons/legal entities convicted for money laundering offences, the number of sentences by type for money laundering offences, etc.

Further development is planned to improve data quality in future collections.

Another important initiative aimed at assessing effectiveness is the "**ECOLEF**" project: the Commission (DG HOME), is currently funding research on the economic and legal effectiveness of the anti-money laundering and combating terrorist financing policy in the European Union under the lead of Utrecht University[162]. It aims at establishing a framework for an encompassing cost benefit analysis for evaluating anti-money laundering and combating terrorist financing (AML-CFT) policy, which includes countries' threat assessments. Its aim is to give financial investigators and policy makers a further sustainable tool to identify and combat ML and TF. The final Report on the ECOLEF project is expected for late 2012.

---

161 ISSN 1977-0375, Eurostat Methodologies and Working Papers, Cynthia Tavares, Geoffrey Thomas and Mickaël Roudaut, 2010 edition.

162 This research is funded by the European Commission's "Prevention of and Fight against Crime (ISEC) Programme (no. of the project JLS/2009/ISEC/AG/087)

ANNEX VIII: COMPARISON OF EU MEMBER STATES' SANCTIONS AND PENALTIES FOR NON-COMPLIANCE WITH AML/CFT RULES[163]

According to article 39 (1) of the AML Directive, Member States shall ensure that natural and legal persons covered by the AML Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive.

Article 39 (2) provides that Member States shall ensure, in conformity with their national law, that the appropriate administrative measures can be taken or administrative sanctions can be imposed against
credit and financial institutions for infringements of the national provisions adopted pursuant to this
Directive. Member States are entitled to impose criminal sanctions, but are however not obliged to
incorporate them into their national legislation.

Member States have transposed article 39 (1) of the AML Directive as follows:

- All Member States have incorporated administrative penalties, as prescribed by article 39 (2) of the AML Directive.
- All Member States have incorporated administrative measures as well.
- Although no obligation exists for Member States to foresee criminal sanctions in case of non-compliance with the national AML legislation, twenty Member States have incorporated criminal sanctions.

Table: Overview of administrative penalties, administrative measures and criminal sanctions in Member States

	Administrative penalties	Administrative measures	Criminal sanctions
Austria (AT)	X	X	-
Belgium (BE)	X	X	-
Bulgaria (BG)	X	X	X
Cyprus (CY)	X	X	-
Czech Republic (CZ)	X	X	X
Denmark (DK)	X	X	X
Estonia (EE)	X	X	X

163 Extract from the study by Consultants Deloitte on the application of the Anti-Money Laundering Directive, Section 3.16: Penalties, January 2011.

Finland (FI)	X	X	X
France (FR)	X	X	X
Germany (DE)	X	X	-
Greece (EL)	X	X	X
Hungary (HU)	X	X	X
Ireland (IE)	X	X	X
Italy (IT)	X	X	X
Latvia (LV)	X	X	-
Lithuania (LT)	X	X	-
Luxembourg (LU)	X	X	X
Malta (MT)	X	X	X
Netherlands (NL)	X	X	X
Poland (PL)	X	X	X
Portugal (PT)	X	X	X
Romania (RO)	X	X	X
Slovenia (SI)	X	X	-
Slovakia (SK)	X	X	X
Spain (ES)	X	X	X
Sweden (SE)	X	X	X
United Kingdom (UK)	X	X	X

Comparability of the penalties

A high level scan of administrative penalties, administrative measures and criminal penalties indicates that penalties throughout Member States are, with the exception of administrative measures, hardly comparable:

- Administrative measures: in general the order for appropriate measures and warning letters are commonly incorporated in the legislation of Member States.
- Administrative penalties: in general two types of administrative penalties are commonly incorporated in the legislation of Member States:
    - Administrative fines: the range in administrative fines is very large e.g. in the Netherlands and in Belgium, fines up to 4.000.000 EUR and EUR 1.250.000 are

possible; in Estonia and Italy, fines can only amount to a maximum of 500.000 croon (31.955 EUR)[164] and 50.000 EUR.
    - Other administrative penalties: the possibility to suspend or revoke a licence and/or impose a public warning are retrieved commonly throughout Member States.
- Criminal sanctions: both imprisonment sentences and/or fines are found throughout the Member States:
    - Imprisonment sentences are foreseen in for example: Denmark, Greece, Hungary, Ireland, Poland, Slovakia, the Netherlands and the United Kingdom. In Slovakia an imprisonment sentence up to 8 years is foreseen in case an unusual business operation was not reported in breach of a person's duty[165].
    - Fines are foreseen in for example: Estonia, Ireland Luxemburg, the Netherlands and the United Kingdom.

Publication and application of penalties in practice

In almost all Member States[166] penalties can be published and therefore penalties can be publicly available.

The publication is however not an automatism due to the fact that:

- In some Member States, the publication must be ordered separately (e.g. Belgium);
- In some Member States, the publication is only performed in case of the most serious infringements (e.g. Italy);
- In some Member States, the publication is directly related to the nature of the sanction itself (e.g. Spain).

Example: publication by separate order of publication (Belgium)

Article 40 AML Law

Without prejudice to other laws or regulations, the competent authority referred to in Article 39 may, in case of non-compliance by institutions or persons referred to in Articles 2, § 1, 3 and 4 of the Articles 7 to 20, 23 to 30 and 33 of this Law, with Regulation No 1781/2006 of the European Parliament and the Council of 15 November 2006 on information on the payer accompanying transfers of funds or with their implementing decrees:

1 ° publish, in accordance with terms it determines, the decisions and measures it shall adopt;

164 As of 1.1.2011, the amount will be set at 32.000 EUR.

165 According to article 234 of the Penal Code.

166 No publication possibilities were reported in Bulgaria, Czech Republic, Germany, Latvia, Slovenia

2 ° impose an administrative fine of not less than 250 EUR and no more than 1.25 million EUR, equal after hearing the defence of the institutions and persons or at least having duly summoned them…

Example: publication only for the most serious infringements (Italy)

Article 57 AML Law

1. Unless the act constitutes a crime, failure to comply with the suspension measure referred to in Article 6(7)(c) shall be punished with a fine of from €5,000 to €200,000.

2. Failure to create the single electronic archive referred to in Article 37 shall be punished with a fine of from €50,000 to €500,000. In the most serious cases, taking account of the gravity of the violation inferred from the circumstances in which it occurred and from the value of the suspicious transaction that was not reported, the provision imposing the sanctions shall be accompanied by an order that the persons fined publish, at their own initiative and cost, the decree imposing the sanction in at least two newspapers distributed nationwide, of which one shall be a financial paper.

3. Failure to set up the customer register referred to in Article 38 or to adopt the recording procedures referred to in Article 39 shall be punished with a fine of from €5,000 to €50,000.

4. Unless the act constitutes a crime, failure to report suspicious transactions shall be punished with a fine of from 1 to 40 per cent of the amount of the non-reported transaction. In the most serious cases, taking account of the gravity of the violation inferred from the circumstances in which it occurred and from the value of the suspicious transaction that was not reported, the provision imposing the sanction shall be accompanied by an order that the persons fined publish, at their own initiative and cost, the decree imposing the sanction in at least two newspapers distributed nationwide, of which one shall be a financial paper.

5. Violations of the disclosure requirements in respect of the FIU shall be punished with a fine of from €5,000 to €50,000.

Example: publication which is directly related to the nature of the sanction (Spain)

Article 56 AML Law

1. For the commission of very serious offences, the following penalties may be imposed:

(a) Public reprimand.

(b) Fine between a minimum of EUR 150,000 and a maximum amount that may be imposed up to the highest of these figures: 5 percent of the net worth of the institution or person covered by this Act, twice the economic substance of the transaction, or EUR 1,500,000.

(c) In the case of institutions requiring administrative authorisation for their operation, withdrawal of this authorisation.

The penalty provided for in point (b), which will be compulsory in all events, shall be imposed simultaneously with one of those listed in points (a) or (c).

2. In addition to the applicable penalty to be imposed on the institution or person covered by this

Act for the commission of very serious offences, one or more of the following penalties may be imposed on those responsible for the offence, having held administrative or management positions in the entity:

(a) Fine for each of between EUR 60,000 and EUR 600,000.

(b) Removal from office, with disqualification from holding administrative or management positions in the same entity for a maximum period of ten years.

(c) Removal from office, with disqualification from holding administrative or management positions in any entity of those covered by this Act for a maximum period of ten years.

The penalty provided for in point (a), which will be compulsory in all events, may be simultaneously imposed with one of those listed in points (b) and (c).

The public availability of penalties in practice is limited. Moreover, throughout our surveys we have noticed that figures on the imposed penalties were practically never provided. Information on the facts on the infringements which gave rise to the penalties is also very scarce.

The fact that penalties are applied in practice is supported by a study from the *Universita Degli Studi di Trento* and the *Universita Cattolica del Sacre Cuore* (2007) [167].

Application in practice was also confirmed by a number of other indications:

- E.g. an Italian public layer sector stakeholder who reported that penalties are applied in practice in 2010. The Italian legal system has an extensive range of (criminal and administrative) sanctions to punish infringements of AML rules.
  The Bank of Italy, as supervisory authority, has made an extensive use of administrative sanctions, both pecuniary and coercive (e.g., prohibitions, bans, etc.), following to controls on supervised entities.

[167] Report on Cost Benefit of Transparency Requirements in the Company/Corporate Field and Banking Sector Relevant for the Fight Against Money Laundering and Other Financial Crime (2007), 103 (available at: http://transcrime.cs.unitn.it/tc/fso/publications/CBA-Study_Final_Report_revised_version.pdf) .

- A desk research on the number of imposed penalties[168] and reports from other stakeholders confirmed as well that penalties are applied in practice throughout Member States[169].

Contrary to the above, the FATF reported with regard to a Member State where (only) a low number of warning letters were sent by the supervisor (supervisor over a very large number of controlled entities) and in the absence of administrative fines, that it is unlikely that there is such a very high level of compliance with AML/CFT measures.

Effect of penalties

Almost all **public layer sector stakeholders** reported that the available sanctions are sufficient and proportionate to the severity of the breach e.g.:

- In **Germany**, a stakeholder emphasized the importance of administrative sanctions and measures for the supervisory authorities.
- In **Hungary**, a stakeholder reported that in its own experience the existing range of sanctions and measures is appropriate to the level of actual threat.
- In **Luxemburg**, it was reported that the severity of the penalties would be increased in a new draft law.
- In **Poland**, a stakeholder reported that penalties should have a deterrent effect and therefore the penalties must be severe. The same stakeholder confirmed that this is the case in Poland.
- In **Portugal**, a stakeholder quoted the background of the national sanctions: the range of sanctions has been proposed by a working group with representatives from the supervisory authorities, the Finance Ministry, the Justice Ministry and the FIU, with the aim to ensure its effectiveness, taking also into due account existing administrative sanctioning regimes.
- In **Slovakia**, a stakeholder reported that the penalties are proportionate and dissuasive as the range of sanctions provides for an adequate supervisory response to the existing legal infringements and cases of non-compliance. In each case the following elements are considered: the severity, if the breach has occurred repeatedly, for how long the law has been violated and all other relevant circumstances.
- In **Slovenia**, it was reported that during the fourth round of Moneyval evaluation it was noted that the level of fines in Slovenia is significantly higher than in many of the surrounding countries (of Slovenia's immediate neighbours only Italy applies higher level of fines for legal persons).
- In the **United Kingdom**, a stakeholder is of the opinion that the range of sanctions available is appropriate and proportionate. Sanctions under the Regulations complement criminal sanctions for the principal money laundering offences in the Proceeds of Crime Act.

[168] A high level scan of recent FATF and Moneyval country reports and recent reports from FIUs was performed.

[169] Hungary (penalties imposed for an amount of 1 100 000 HUF in 2009), Slovakia (30 imposed penalties in 2009), Sweden (in 2008: 2 banks were sanctioned with a fine of 50 million SEK for major non-compliance, source FATF report Sweden 2010, p. 14) Poland (16.000 PLN in 2010), Romania (Non financial banking institutions – 200 000 RON; Companies – 50 000 RON, Real estate sector – 37 000 RON Auditors – 15.000 RON in the period 2009-2010).

Covered entities who gave an opinion on this matter (all non-financial professions) clearly have different views. Some stakeholders indicated that the available sanctions are not proportionate to the severity of the breach. Others have indicated the opposite.

- In **Germany** and in **Cyprus**, stakeholders reported that due to the wide range of administrative sanctions, a suitable penalty can be imposed in every case.
- In **Ireland,** a stakeholder reported that it considers the sanctions to be excessive in the relation professional - client;
- In **Poland**, a stakeholder reported that the sanctions are certainly dissuasive due to the disproportionate criminal sanctions;
- In **Spain**, a stakeholder reported that the sanctions are extremely severe;
- In the **United Kingdom**, different stakeholders commented on the existing criminal sanctions expressing the opinion that the criminal sanctions are disproportionate. Some respondents question the fact whether the regime itself has led to more convictions of principal offenders.

In a very recent report from HM Treasury (United Kingdom)[170] on the review of money laundering regulation, the following was stated regarding the effect of criminal sanctions:

"Many believe that the threat of a criminal penalty under the Regulations discourages a risk based approach and encourages businesses and Money Laundering Reporting Officers to adopt a zero tolerance policy. However there some responses make the case for the continued provision of a criminal penalty, including the deterrence effect and the opportunities provided for supervisory and law enforcement activity."

[170] Review of the Money Laundering Regulations: summary of the call for evidence (March 2010) – HM Treasury, p. 12

ANNEX IX: COMPARISON OF EU MEMBER STATES' RULES IMPLEMENTING AML RULES TO CASINOS AND THE GAMBLING SECTOR

Obligations only upon casino operators	Obligations upon casino operators and other gambling operators
Austria	**Bulgaria** (*Casinos, bingo halls, lotteries, sport totalizators, etc.*)
Belgium	**Estonia** ("*Organizers of games of chance"*)
Czech Republic	**Finland** ("*Any gaming operator and supplier of gaming activities"*)
Germany	**Greece** (*"Casino enterprises, casinos operating on Greek ships, companies, organizations and other entities engaged in gambling activities as well as betting shops (agencies)").*
Hungary	**France** (*Casinos, clubs, groups or companies in charge of games of chance, lotteries, betting, sport and horse race forecasts)*
Malta	**Ireland** (*Casinos and private members' clubs*)
Romania	**Italy** (Land based and online *casinos, sport betting/forecasts and other gambling activities*)(*Casinos, online sport betting/forecasts*)
The Netherlands	**Latvia** (*Lotteries and gambling*)
United-Kingdom	**Lithuania** (*"Companies offering gaming")*
	Luxembourg (*"Casinos and similar premises"*)
	Portugal (*Casinos, betting and lottery operators)*
	Slovenia (*Casinos, gaming halls, sport wagers, online games of chance*)
	Spain (*Casinos, lotteries and other games of chance*)
	Sweden (*Casinos, lotteries and other games of chance*)

Source: Altius